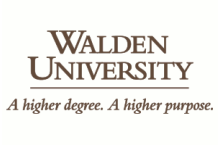


2020

Obstacles With Data Security: Strategies From Carolina Universities

Yamiah R. Compton
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Yamiah Compton

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Gary Griffith, Committee Chairperson, Information Technology Faculty
Dr. Bob Duhainy, Committee Member, Information Technology Faculty
Dr. Steven Case, University Reviewer, Information Technology Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2020

Abstract

Obstacles With Data Security: Strategies From Carolina Universities

by

Yamiah Reneé Compton

MSIT, Walden University, 2016

MSCJ, Tiffin University, 2014

BS, Purdue University, 2009

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

August 2020

Abstract

Some university data custodians lack information security strategies to prevent data security breaches. Reducing duplicitous use of personally identifiable information (PII) obtained maliciously from colleges and universities should be important to university data custodians, IT leadership of all levels, state legislators, and individuals that have an interest in moving into the cybersecurity space in higher education. Grounded in general systems theory, the purpose of this multiple qualitative case study was to examine information security strategies that university data custodians use to protect PII collected from staff, students, and other stakeholders. The participants consisted of 15 college and university data custodians in North Carolina and South Carolina, who implemented security strategies. Semistructured virtual interviews were used to collect data. The verbatim transcripts were analyzed using thematic analysis in conjunction with Tesch's data coding process then compared to current literature as a control. There were 5 key emergent themes (a) adaptive security measures, (b) necessity for buy-in resources, or both (c) proper management and personnel, (d) requirements based on state/industry regulations, and (e) security education training and awareness. University data custodians should implement, promote, and monitor comprehensive information security strategies to protect university PII. The implications for positive social change include potential leadership awareness to protect university PII and minimize the adverse effects of a data breach.

Obstacles With Data Security: Strategies From Carolina Universities

by

Yamiah Reneé Compton

MSIT, Walden University, 2016

MSCJ, Tiffin University, 2014

BS, Purdue University, 2009

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

August 2020

Dedication

I would like to dedicate this study to my family and friends. My parents, Teresa and Darrell Compton, have pushed me since the very beginning to finish what I start. They are my foundation. My grandmother, Sandra Norman, never failed to give me all the encouragement I needed to make it through this program. She is my inspiration. My siblings, De'Onte, Marcus, Filoi, Keneshia, and Kendra, all held me accountable for setting an example as the older sister. They are my motivation. My ships (Hakeenah, Jessica, Tiffanie, and Charlisa) as well as my sister-friends (Casey, Netanjea, Reva, Kim Moorehead, and Kim Moore) continuously gave me a shoulder to cry on and always lent me a listening ear. They are my blessings. My support system is unrivaled and I thank each and every person in it, mentioned or not, from the bottom of my heart.

Acknowledgments

I would like to acknowledge the guidance I received from my chair Dr. Gary Griffith, my second committee member Dr. Bob Duhainy, and my university research reviewer, Dr. Steven Case. With their support, I am finally able to close this chapter in my life and start a new one among the ranks of the 2%. I sincerely thank them, as well as the other professors in the College of Management and Technology who laid the foundation for me to successfully complete the doctoral study portion of this program.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Colleges and universities house millions of records containing personal information about staff, students, alumni, and various stakeholders. Data breaches are a growing problem (Elhai & Hall, 2015) that affects more than just the government, financial institutions, and major retailers. Breaches within colleges and universities can potentially impact millions when data is not properly secured. This section provides the background of the problem and the purpose of the study.

Background of the Problem

A data custodian is an individual or group of individuals that collects, manages, and stores data collected for various reasons and is held accountable for data distribution (Smith et al., 2015). One major issue with data security as a concept is that there is no single well-rounded approach to examine data security as a complete systematic organism (Akram & Ko, 2014). This leaves room for holes in information security policies, thus leaving vulnerabilities in the protection efforts of the data custodian. Therefore, examining the information security strategies that university data custodians use to protect personal information collected from staff, students, and other stakeholders is obligatory.

Securing information provided to the college or university with the understanding that it will be safe should not be a far-fetched concept. As of late, this concept seems to depart further and further from reality. Examining information security strategies already implemented in a college or university can open a window of opportunity for the information technology (IT) field. This examination can help determine where the problem lies and how to address it.

Problem Statement

In March 2018, nine Iranian hackers were indicted under charges of stealing university data from at least 144 U.S. universities (Grabosky, 2018). Colleges and universities are not sufficiently addressing the issue of information security threats, resulting in education-sector breaches more than doubling from 2016 to 2017 (Rodriguez, 2018). The general IT problem is that the number of data breaches at the university and college level is increasing. The specific IT problem is that some university data custodians lack information security strategies to protect personally identifiable information (PII) collected from staff, students, and other stakeholders.

Purpose Statement

The purpose of this qualitative case study was to examine the information security strategies that university data custodians use to protect PII collected from staff, students, and other stakeholders. The original targeted population consisted of data custodians from 30 universities in North Carolina and South Carolina that have implemented a set of security strategies. The implication for positive social change was that improved security strategies have the potential to minimize the chances of identity theft or any other negative side effect of a data breach involving Carolinians affiliated with universities.

Nature of the Study

The qualitative methodology was used for this study after considering each of the three possible research approaches: qualitative, quantitative, and mixed methodologies. Qualitative methodology is used when something is not well defined and needs exploration, the problem is complex and requires description, the context of a problem calls for in-depth observation, there is a necessity to explain linkage, and when measurement is not particularly warranted (Yakhnich, 2016). Qualitative methodology was chosen based on this reasoning because this research sought

to discover a way to mitigate the number of data breaches that occur at colleges and universities. In this research, I also explored a complex problem, improving security strategies, which is comprised of several linked components, all of which led to the decision to apply the qualitative method to this study. Quantitative research is generally used when testing theories that are already constructed (Mehrez, 2013) or to examine the possible relationship between variables (Mahanani, 2018). This study did not set out to test a theory that has already been constructed nor are there any variables involved. Mixed-methods research is a combination of qualitative and quantitative methodologies (Halcomb & Hickman, 2015) and was not appropriate as the quantitative component did not apply to this study.

Case study, ethnographic, narrative research, and phenomenological designs were the viable options for this qualitative study. Scholars using the case study design seek to investigate a problem in its natural context with one or more cases (Shaw, 2013). The case-study design was used in this research to examine information security strategies used by data custodians in the natural context at different universities. Ethnography is defined as the science of depicting a culture (Lanclos & Asher, 2016). Ethnography is best suited for providing descriptions of people's experiences and answering the why and how about cultural practices (Lanclos & Asher, 2016). This study looked at the security strategies being used to protect data, not at the social or cultural practices in universities or among data custodians. Narrative research provides individual stories for development (Lewis, 2015). Narrative research was not chosen as there are no stories to examine, only information security strategies. Phenomenological studies investigate the lived experience of a given phenomenon (Percy, Kostere, & Kostere, 2015). Phenomenological design, although considered at the primary stages of this study, was not chosen because the primary focus of this study was not the lived experiences of data custodians.

Research Question

What information security strategies do university data custodians use to protect PII collected from staff, students, and other stakeholders?

Interview/Survey Questions

Demographic Questions

1. What is your current title and role/responsibilities at the university?

2. What role do you have in providing data security for the institution?

3. How long have you been providing data security for the university? For any institution?

4. What applicable data security certifications and/or training have you had or plan to obtain?

Interview Questions

1. What training is given to data custodians to aid in ensuring proper data security?

2. Does your university develop security strategies based on a particular framework or standard?

3. Does your university have a centralized or decentralized management structure for data custodians across campus?

4. Were you involved in the process for choosing which person(s) modify the implemented security strategies? If so, what is that process?

5. How have other university data breaches caused this university to amend its existing security strategies in the past 5 to 10 years?

6. In your experience, which security strategies have been the most beneficial in providing data security for the university? Why have they been the most beneficial?

7. How often are the university's security strategies updated?

8. What prompted the implementation of the security strategies that exist within the university today?

9. What external factors play a role in deciding what strategies to implement within the university? Do these external influences cause challenges or make it easier to implement these strategies?

10. What method is used to measure the effectiveness of the security strategies? Is this method used before, after, or throughout implementation?

11. Do you have any additional information to provide surrounding security strategy implementation at the university that has not already been addressed?

Conceptual Framework

The conceptual framework that informed this study and allowed examination of the strategies that university data custodians use to protect collected PII was the general systems theory (GST). Karl Ludwig von Bertalanffy (1950) was the father of this theory and its concepts. Von Bertalanffy first presented ideas about this theory in the field of biology after World War I in the 1920s (Iwu, Kapondoro, Twum-Darko, & Lose, 2016). GST is a general, yet complex, theory that consists of three aspects: systems science, systems technology, and systems philosophy (von Bertalanffy, 1972). The aspect of this theory that most apparently applied to this study was systems technology. *Systems technology* refers to issues discovered within hardware and software during everyday use involving modern technology and the public, such as data breaches, identity

theft, and system hacking (von Bertalanffy, 1972). Systems science is simply the exploration of systems in relation to the diverse sciences that include, but are not limited to, technology, psychology, engineering, and economics, whereas systems philosophy follows the thought process after the presentation of a novel architype (von Bertalanffy, 1972).

GST is used to view organizations as systems with interrelated subsections that must coexist in a conflict-free nature to be effective (Teece, 2018). Viewing a college or university as a system and information security as a subsection of the system, I applied GST to this study to examine information security strategies within the university. GST provided a framework that allowed the exploration of the relationships between information security, implementing security strategies in the university, and compliance with the implemented strategies within the university. Through this exploration, I discovered strategies and broadcasted discoveries about the significant themes of those strategies.

Definition of Terms

Chief information security officer: A dedicated security team—preferably led by a chief information security officer—has full, centralized control over policy and implementation, enabling the business to achieve uniform security across the entire enterprise, rather than the fragmented, even contradictory, solutions often deployed on a departmental basis (Boone, 2017).

Data breach: An incident that encompasses unsanctioned access to confidential, protected, or sensitive data, thus ensuing the possible, or actual, compromise of either availability, confidentiality, or integrity of said data (Rosati, Deeney, Cummins, van der Werff, & Lynn, 2019).

Data custodian: An individual or group of individuals that collect, manage, and store data collected for various reasons and would be held accountable for data distribution (Smith et al., 2015).

Data security: The strategic process used to protect data from destructive forces or from unauthorized access, also known as a *data breach* (Mahmoud, Seyed, & Hon, 2016).

Information assurance: Information procedures that defend data and its systems by guaranteeing their availability, integrity, authentication, and confidentiality, which includes the incorporation of protection, detection, and reaction capabilities (Khorana, Ferguson-Boucher, & Kerr, 2015).

Information security policy (ISP): The National Institute of Standards and Technology (NIST) defines an ISP as a combination of directions, guidelines, rules, and practices that suggests how an organization should manage, protect, and issue information (Da Veiga, 2016).

Needs assessment: Process used to categorize and prioritize structural gaps to create better quality programs (Iannuzzi, Grant, Corriveau, Boissy, & Michaud, 2016).

Personally identifiable information (PII): Information that can be used to differentiate or discover an individual's identity (O'Neill, Dexter, & Zhang, 2016).

Security education training and awareness (SETA) program: An educational procedure through which employees satisfy the essential conditions for information security (Han, Kim, & Kim, 2017).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are the rudimentary basis of research for scholars and can be regarded as a concept the scholar accepts as true without concrete proof (Dean, 2014). Two assumptions guided the data collection and analysis strategies for this study. The first assumption was that the university data custodian understood fully what it takes to protect the university data they maintain. One major issue with data security as a concept is that there is no single well-rounded approach to examine data security as a complete systematic organism (Akram & Ko, 2014). This leaves room for holes in the ISP, thus leaving vulnerabilities in the protection efforts of the data custodian. As long as the data custodian understands this concept and has taken the proper precautions to address the issue, the information gathered should be accurate. There was no way to provide concrete proof of comprehensive understanding.

The second research assumption concerned the classification of the data collected and protected by the data custodian. If the information gathered by the data custodian is not properly classified, there would be no real way to set a comprehensive ISP to protect the data. With properly classified data, the data custodian can look at the information in hand and determine the ways the data can, and should, be properly organized, disseminated, and stored. For example, a nine-digit number can be stored and classified as an extended ZIP code without masking, but a nine-digit number stored and classified as a social security number should have proper masking. If this is not classified properly, information can be leaked with ease.

Limitations

Limitations of a study are defined as circumstances that have the capability of deteriorating or constraining deductions that may be drawn from the research (Beebe, 2004). One

of the limitations of this study was that all participants targeted may not have the breadth of knowledge needed to give adequate information. Data custodians are individuals who deliver and maintain computing resources for hosting and processing collected data (Aljumaili, Wandt, Karim, & Tretten, 2015). Although data custodians are professionals, without their levels of knowledge being researched, there was no way to determine the actual amount of knowledge they had about their position.

The second limitation of this study was that the study findings may not be generalized for all the United States due to the case study focusing on institutions of higher education in the Carolinas. The findings may, however, be applicable to other states. Case studies have an inherent limitation of generalizing (Leung, Leung, & Yuen, 2016). Case studies also present the limitation of transferability. Case studies present a unique subset of ideas to the reader. It is then up to the reader to decide if the generalized information presented is appropriate for comprehensive understanding of similar instances. Given these innate limitations, I believed the information in this study was able to add value to the literature and to the field of IT.

Delimitations

Delimitations of a study address the scope of the research and how it will be focused (Beebe, 2004). The first delimiter of this study was the geographical location of the study. University data breaches are not exclusive to the Carolinas; however, the geographical location of the study was centered in the Carolinas. The second delimiter placed on this study rested in the choice to only examine universities/colleges and no other facilities. The final delimitation in this study was the given security strategy implemented as they varied within each institution as not all data custodians used the same concepts and constraints for implementation.

Significance of the Study

Contribution to Information Technology Practice

This study may be of value to universities, specifically data custodians and the individual's private data belongs to. This is due to the increasing number of university data breaches. If data custodians can have a better grasp of the strategies required to minimize or completely stop the number of breaches that occur annually, this would be tremendously effective.

This study may contribute to the improvement of IT practice by aiding in the establishment of a baseline strategy for securing data. Although data custodians at universities were the target in this study, the results may be applied to other noneducational sectors. For example, any formulated security strategies implemented by data custodians in the education sector could also be used by IT specialists in the government sector. In this study, I examined IT strategies that could be tailored for any IT professional to aid in the protection of PII.

Implications for Social Change

The implication for positive social change is that improved security strategies may have the potential to minimize the chances of identity theft or any other negative effects of a data breach involving Carolinians affiliated with universities. The results also have the potential to make IT professionals, such as data custodians and chief information security officers aware of the lack of efficiency in existing policies.

A Review of the Professional and Academic Literature

The purpose of this qualitative case study was to examine the information security strategies that university data custodians use to protect PII collected from staff, students, and other stakeholders. The objective of this academic literature review was to provide a

comprehensive critical analysis and synthesis of various content of the literature. This academic review has been subdivided into sections that explicate (a) GST, (b) applications of information security, (c) aspects of data breaches, and (d) the gap in academic literature.

This academic literature review consists of 80 articles from various academic journals. Of the 80 articles, 68 (85%) are peer reviewed and 70 (87.5%) have a publication date less than 5 years from the anticipated CAO approval date. This subset of articles was mainly retrieved from EBSCOhost, ProQuest Central, Google Scholar, Academic Search Complete, ScienceDirect, and the Walden University library. Ulrich's Web was used to verify both the validity of the journals in respect to the articles being peer reviewed. The search criteria included the following keywords: *data breach, information security, security policies, ISPs, personal identifiable information, PII, college and universities, security strategies, SETA, general systems theory, GST, systematic evaluation, InfoSec, systems theory, chaos theory, high reliability theory, cybernetics, data, breach, data loss, security, data theft, colleges, universities, hacking, conceptual model, regulations, security education, data custodians, reductionism, Newtonian science, litigation,* and *history and security incidents*.

General Systems Theory

I chose GST for this study after a comprehensive critical analysis of the literature addressing the research question that set out to examine the information security strategies that data custodians use to protect PII from breaches. Von Bertalanffy was the father of this theory and its concepts. GST is a general, yet complex, theory that consists of three aspects: systems science, systems technology, and systems philosophy (von Bertalanffy, 1972). The aspect of this theory that most apparently applied to this study was systems technology. Systems technology refers to issues discovered within hardware and software during everyday use involving modern

technology and the public such as data breaches, identity theft, and system hacking (von Bertalanffy, 1972). Systems science is simply the exploration of systems in relation to the diverse sciences that include, but are not limited to, technology, psychology, engineering, and economics. Systems philosophy follows the thought process after the presentation of a novel archetype (von Bertalanffy, 1972).

Three of the most prominent principles of GST directly related to this study are the boundary principle, the hierarchy principle, and the holism principle (Whitney, Bradley, Baugh, & Chesterman, 2015). The boundary principle indicates that the perimeter of a system describes the pieces that make up a system and separate those pieces from different factors, preventing entry of information (Whitney et al., 2015). The boundaries for this study could be several components including the physical computer that contains the data, the database that houses the information outsiders want to obtain, or the security system set up to keep intruders out and information in. The hierarchy principle proposes that objects treated as a whole are made up of smaller objects, which are to be regarded as wholes in themselves (Whitney et al., 2015). A security strategy is a document made of many steps that address individual concerns that affect the whole, while each concern is a whole object itself. Finally, the holism principle states that a system should be regarded as a whole, not as a summation of individual parts (Whitney et al., 2015). This is different from the hierarchy principle, but it allows the decision maker to take a different approach and perspective for solving any issues within the system. The two concepts most relevant to this study were the centrality axiom and the contextual axiom (Whitney et al., 2015). The centrality axiom is supported by the hierarchy principle and states that the levels in a system's hierarchy are based on the development of sublevels (Whitney et al., 2015). The contextual concept is supported by both the boundary and holism principles stating that the

meaning of a system is defined by factors surrounding the system (Whitney et al., 2015). Each of these principles and concepts can be directly applied to and supported by this study.

Systems-based approaches when referring to complex situations involving decision making enable the decision makers to address the situation fully (Yurtseven & Buchanan, 2016). The goal of GST is to methodically determine a system's inner workings, such as subtleties, restrictions, conditions, and ideologies that can be distinguished and applied to systems on various levels. Von Bertalanffy (1972) formulated GST to be applied to all systems in different fields of science due to the underlying belief that all systems are similar (Kordova, Frank, & Miller, 2018). Applying GST in one scientific field can help remedy issues and explain occurrences in other fields (Kordova et al., 2018). With data breaches, humans (i.e., data custodians) are responsible for protecting data saved on computers (i.e., technology). GST offers a commanding lens to examine a vast range of phenomena involving both humans and technology (Chatterjee, Xiao, Elbanna, & Saker, 2017).

Many of the concepts of GST were used in management and information systems while being classified as either system dynamics, management cybernetics, systems engineering, or the systems approach (Mingers, 2017). GST was used in this study as the conceptual framework to delve into the correlation between data custodians, security strategies and the implementation of security strategies at various colleges and universities. Data breaches are the complex situations, decision makers are the data custodians, and security strategies are the interrelated components that must be implemented to assist with solving the complex situation. Given this understanding of the components, it is easy to see why GST was used as the framework for this study.

The evolution of general systems theory. The roots of systems theory can be traced back as far as Aristotle with the promotion of one of the prominent GST principles of holism

(Iwu et al., 2016). In modern times, the concepts of GST were developed in the early 20th century in various disciplines (Mingers, 2017). Von Bertalanffy is credited with coining ideas about this theory in the field of biology after World War I (Iwu et al., 2016). He originally defined a system as a group of everchanging components that maintains its integrity through mutual interactions (Ceric, 2015). He applied the definition when he needed to justify the relationships of living organisms (Iwu et al., 2016). The theory was formally established in the 1930s and advanced by the 1970s by scholars including Gordon Pask, Ross Ashby, Anatol Rapoport, Margart Mead, Kenneth Boulding, and many others (Caws, 2015; Rousseau, Wilby, Billingham, & Blachfellner, 2016; von Bertalanffy, 1972). In 1954, the International Society for the Systems Sciences was established under the name of the Society for the Advancement of General Systems Theory and was incorporated in 1956 as the Society for General Systems Research (Drack & Pouvreau, 2015; Rousseau, 2015). GST founders felt that this theory would assist with closing the divide between object- and subject-oriented disciplines (Rousseau, 2015). Seminal scholars, including Wolfgang Kohler, Alfred Lotka, and Vito Volterra, have contributed to this theory as well (von Bertalanffy, 1972).

GST is not a directory of equations and solutions (von Bertalanffy, 2008). This theory is used as a device in science that acts as a means of regulating the transfer of principles from one scientific field to another, eliminating the need for redundant principle discovery in the different scientific fields (von Bertalanffy, 2008). Two concepts that have evolved GST and that are transferable between scientific fields are open systems and closed systems. Scholars, such as Wertz, Reiner, Denbigh, Prigogine, and Wiame, have contributed to the development of these concepts in various scientific fields (von Bertalanffy, 2008). Open systems have an inward and outward flow, thus altering the component makeup (von Bertalanffy, 2008). Closed systems are just the opposite of open in that no components flow in or out. Open systems are malleable and

have permeable boundaries whereas closed systems do not (Chatterjee et al., 2017). Open systems do not have a limit on the number of ways they can be opened, and those systems can become closed using selective elements making the extent of a system a matter of choice (Caws, 2015). Business organizations, such as colleges and universities, are generally described as open systems when discussed in the literature (Iwu et al., 2016). The scope has been narrowed for this study, but sometimes the scope is all-encompassing, leaving room for missing contingencies, which comes with huge consequences for human welfare such as data landing in the hands of the wrong person because of a data breach (Caws, 2015). The main components of a system are the inputs, outputs, processes, subsystems, and feedback (Iwu et al., 2016). Business organizations gain resources (or inputs) and route them using a business process (or strategy) to produce a service as an output (Iwu et al., 2016). In this study, I examined the portion of the subsystem that addresses this strategy.

Many models have been informed by GST, including the systematic evaluation model. The systematic evaluation model, also referred to as the SUV model, was developed at the eHealth Institute at the University of Kalmar in Sweden (Jokela, Karlsudd, & Östlund, 2008). This model takes a systems-based approach and is derived from GST. It consists of three levels—(a) individual, (b) technology, and (c) organization—and seven categories—(a) goal seeking, (b) regulation, (c) hierarchy and relations, (d) differentiation and entropy, (e) transformation process, (f) input, and (g) outputs (Jokela et al., 2008). Each of the three levels also contains the seven categories (Figure 1). This model was used to construct questions for the participant interview.

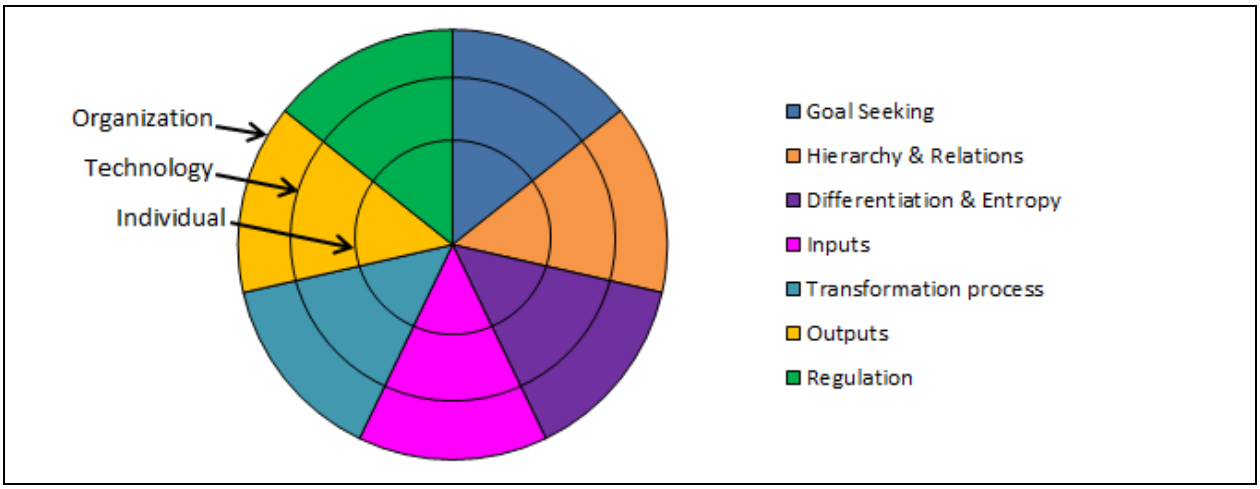


Figure 1. Systematic evaluation model depicting the seven categories and three levels used for question development. Adapted from "Theory, method, and tools for evaluation using a systems-based approach," by P. Jokela, P. Karsudd, and M. Östlund, 2008, *Electronic Journal of Information Systems Evaluation, 11*, p. 200. Copyright 2008 by Jokela et al. Reprinted with permission (see Appendix C).

The primary construction of GST was in the form of a theoretical science mainly geared at researching systems and their common features (Ceric, 2015). GST has evolved and is still being evolved today. For example, Rousseau (2015) called for the transdisciplinary general systemology to be a branch of GST, which Rousseau suggested should further be labeled as GST* (Rousseau et al., 2016). Malecic (2017) questioned Rousseau's proposal, but did indicate that GST does have issues with its own definition so evolution in GST was more than likely going to continue. Malecic also confirmed that the difference between systems science and regular science is transdisciplinarity (Malecic, 2017). GST currently has a wide variety of meanings and translations (Rousseau et al., 2016). Given the polysemous nature of general systems theory, GST has been linked to several different theories both in a supporting and a contrasting role usually based on the interpretation of the scholar invoking the idea. A couple of the supporting theories are high reliability theory and chaos theory. Newtonian science and reductionism, on the other hand, have been noted as contrasting, or rival, theories to GST.

Theories that support general systems theory. With the number of years that general systems theory has been relevant in the sciences, it would be considered normal and accepted to have a few theories that have been informed by GST, in turn supporting the theory's aims and precepts. When examining the literature to develop this review, two theories stood out more than others as they were mentioned in books, journal articles and dissertations on a regular basis. High reliability theory and chaos theory have been applied to several studies and have been linked back to general systems theory in several ways. There have also been links from high reliability theory and chaos theory to security strategies and data breaches in various organizations.

High reliability theory. Todd La Porte, 1987, is one of the founders of high reliability theory (HRT; Shrivastava, Sonpar, & Pazzaglia, 2009). HRT was developed on the campus of University of California, Berkeley by scholars that studied how organizations that used complex technologies managed to remain without incident while still maintaining quality and meeting arduous goals (Shrivastava et al., 2009). According to Shrivastava et al. (2009), it took several years for scholars to agree on the definition of reliability as the ability to operate and complete operations without an error even though the definition was not explicit. This study sets out to examine the security strategies, or processes, that data custodians use to protect data from data breaches. HRT could have been used as the conceptual framework for this study because in an organization, reliability is a result of proper management of fluctuations, shifting the emphasis from routines to processes (Shrivastava et al., 2009).

HRT supports GST in several ways. One major way that HRT and GST relate is the lens used to examine an issue. Both have been used to examine IT projects by exploring an organization and its operations to determine how it effects the final result (Saunders, Gale, &

Sherry, 2016). Another way that HRT and GST relate involves the type of systems that each address. Both theories address complex, open systems where arising issues are inevitable while using a more optimistic view to examine and categorize said systems (Bergstrom, van Winsen, & Henriqson, 2015; Saunders et al., 2016). Although HRT relates to GST in various ways, ultimately GST was chosen instead because HRT applies more to the safety concept in organizations that deal in hazardous areas such as power plants (Bergstrom et al., 2015).

Chaos theory. Henry Poincare's study of sensitivity to physical systems' initial conditions marked the beginning of chaos theory (Kesić, 2016). Edward Lorenz, 1963, a mathematician and a product of the Massachusetts Institute of Technology, is credited as the founder of chaos theory (Oestreicher, 2007). The term chaos theory was not actually applied to this view until 1975 by mathematician James A. Yorke (Oestreicher, 2007). The mathematical chaos theory allows for the description of a subset of phenomena within the field that is concerned with the effect of forces on the movement of an object (Oestreicher, 2007). Chaos theory, which later became complexity theory, emerged when the hard sciences began making assumptions about systems that later were not found to be true (Mingers, 2017). Chaos theory could have been used as the conceptual framework for this study since the theory had been combined with elements of GST in the past to evaluate complex systems (Teece, 2018). Chaos theory and GST both focus on dynamic systems that use a set of equations to measure how systems change over a period of time (Kesić, 2016).

Chaos theory supports GST in relation to the shared concepts and usages between the two. Feedback, or an answer to presented information that either has a positive or negative charge, is listed as a concept of both theories (Oestreicher, 2007). Chaos theory has also been used to expand the application of GST. When combined with chaos theory, GST can be used by

management scholars to better address high complexity systems (Teece, 2018). Although chaos theory relates to GST in various ways, ultimately GST was chosen instead since chaos theory applied more to time, space, and other notions of mathematical proportions (Oestreicher, 2007).

Theories that rival general systems theory. For every positive, there must be a negative. When a theory is developed, it would be considered normal and accepted to have a few theorists that have studied the theory and challenged the viewpoint rivaling the theory's aims and precepts. When examining the literature, it was quite difficult to find theories that rival GST. Newtonian science and reductionism were two theories that appeared to rival GST in the form of usage and drawn conclusions.

Newtonian science. There is an innate contradiction between the old way and the new way of thinking which lies as the root cause from the contrast between the paradigm of complexity and the paradigm of complication (Daniel & Daniel, 2018). As mentioned before, GST addresses high complexity systems. Newtonian science is usually contrasted with GST because of this concept. Newtonian science falls into the paradigm of complication (Daniel & Daniel, 2018). Newtonian science is viewed as more traditional and linear making many researchers in the science field want to move beyond this classic mind set and into a mindset that is more dynamic (van de Wetering, Mikalef, & Helms, 2017). There are several documents that have been released within the science field that Newtonian science to reductionism. Newtonian science is based on reductionism, thus making the theory a direct rival of GST as well (Daniel & Daniel, 2018).

Reductionism. Reductionism and GST operate on opposite ends of the theoretical spectrum with reductionism stating that an issue or project can be broken into parts to be reviewed and GST stating that dynamic and complex issues should be reviewed as a whole

(Chen, 2016). Reductionism operates on the premise that science is supposed to take a given set of variables and identify, isolate, and assess the relationship amongst that set (Chen, 2016). Reductionism holds that the characteristics that explain the behavior of a system are linear, predictable, and deterministic in nature while GST insists that the behavior is nonlinear, sensitive to conditions and chaotic in nature (Kesić, 2016). In the 1980s, GST's key principle of holism allowed scientists to see that reductionism was not adequate for the use in understanding a complex system (du Pisani, 2018).

Reductionism and GST both have theories of program and theories of evaluation. Chen (2016) identifies the theories of program, the theories of evaluation, the advantages of applying each, as well as the challenges. This comparison truly sets the tone for the rivaling foundations of each theory. Reductionist theories of program set out to label components that are essential in understanding effectiveness (Chen, 2016). Reductionist theories of evaluation attempt to give evidence for a relationship outside of influence from alternate factors (Chen, 2016). Rigor of evaluation, enhancing scientific reputation and acting as a basis for movement are some of the advantages while abandoning complexity, ignoring practical issues, and generalizing efficacy are some of the challenges (Chen, 2016). On the opposite end of the spectrum, theories of program applicable to GST examine interaction links to understand a system and theories of evaluation inspect links among components of a complete system to measure the intended, or unintended, final result (Chen, 2016). Providing thorough explanations, facilitating collaboration, and detecting synergies and behaviors are some of the advantages while relying on other theories, information overload, and difficulties with data are some of the challenges (Chen, 2016). There are glaring differences between the two theories making it easy to see why they are common rivals of one another.

Applications of general systems theory. GST was birthed in the scientific field of biology and has since been applied in most every field to include management, information technology, information security, economics, transportation, and leadership. Being that GST is extremely broad in nature, the theory can be applied in various ways to assist scholars with completing their research. The following information gave life to the ways in which the GST lens has been applied scholastically over the years.

Strategic human resource. Iwu et al. (2016) used GST to show that strategic human resource metrics (HRM) should be able to understand and interpret any relationship between human resource outcomes and performance criteria (i.e., profitability, quality, and customer service). Using GST, the scholars were able to deduce that attitudinal HRM results thrive as functional variables that makes up a subsystem that could possibly be associated with superior employee performance (Iwu et al., 2016). The scholars cited several studies that provide evidence of an association between performance and HRM outcomes (Iwu et al., 2016). A general systems concept and conceptual framework were mapped out to show the relevant subsystems that were used for analysis of the listed hypothesis, a four-section questionnaire was used to collect data and conclusions were drawn based on the gathered information. The conclusion of the strategic human resource study showed that GST directly resonated in the problem conceptualization, research philosophy, design, methodology, and analysis of the results (Iwu et al., 2016).

Information technology assets. Wang, Shi, Nevo, Li, and Chen (2015) applied GST in tandem with resource-based view in their study to examine IT assets' business value within different degrees of environmental dynamism and how they improve the performance of a firm. The scholars cited studies dating back to 1997 that provided key findings on relationship configurations as well as performance in isolation, but it was stated that their knowledge is

incomplete based on the research provided since none looked at this matter from a systems perspective (Wang et al., 2015). This is what sparked the interest in doing the study as there was a gap in literature. Four hypotheses were drawn, questionnaires were used to gather data, and conclusions were drawn based on the gathered information. The conclusion of the information technology asset study showed that IT assets do not directly impact firm performance, but other findings were made that could improve IT management and possibly would not have been discovered without adopting the GST perspective (Wang et al., 2015).

Information security. Anton and Nedelcu (2015) applied GST to examine information protection directly related to risk in an integrated information security system and its relation to cost. These scholars used their study mainly to define and describe risk. A diagram of an overall control loop as well as a graphical representation for attitude towards risk was presented to the audience to further the scholars' explanation (Anton & Nedelcu., 2015). Their study was important to mention as it touches on another aspect of GST being used to address an information security (InfoSec) issue. Just as this study addressed, the scholars' study mentioned that IT managers are aware that long-term security is the ideal achievement and that it is difficult to attain the actual financial cost of improper ISPs, mostly due to the varying nature of the fields, impacts and accuracy (Anton & Nedelcu., 2015). The conclusion of their study showed that each person has a differing perspective of risk based on varying factors including, but not limited to, goals, job title and their background, and that the associated cost of a risk is directly related to the weight of the function (Anton & Nedelcu., 2015).

Building information modeling. Oesterreich and Teuteberg (2018) used GST to examine the relationship between cost and benefit suggestions stemming from building information modelling (BIM) investments. Even with the dozen studies cited in reference for their

study, the scholars identified a research gap and used their study as an opportunity to begin closing the gap by providing another perspective for BIM studies (Oesterreich & Teuteberg, 2018). A cost-benefit analysis was completed, a quantification model was developed based on the analysis and several stock flow diagrams were presented to compare different elements of BIM. The conclusion of their study states that BIM investments are valuable for an organization even though the simulation model only shows one situation in relation to BIM's financial impacts (Oesterreich & Teuteberg, 2018). By applying GST to their study, the scholars were able to give an enhanced view of the environment and show how accost-benefit analysis can be used more effectively to aid in the decision making process (Oesterreich & Teuteberg, 2018).

Fractal fluctuations. Selvam (2015) used GST to examine the inverse power law form of fractal fluctuations. It would make sense that GST could be applied to Selvam's study as GST's birthplace was in the scientific field of biology and examined biological systems. There were no past studies presented in this study, but there were several calculations mentioned that referred to other studies for their origin. A GST model for predictions in the space-time fractal fluctuation pattern of systems was presented to better illustrate the scholar's point of view (Selvam, 2015). This quantitative study concluded that while a majority of DNA does not code for proteins, most of it is biologically important enough to survive and continue during the evolutionary phase (Selvam, 2015). Selvam's study was very complex and GST was used throughout to model the scholar's thoughts and processes.

Road safety. Hughes, Newstead, Anund, Shu, and Falkmer (2015) used GST to further analyze road safety strategies. Their study was important to mention as it touches on another aspect of GST being used to address security strategies. The scholars' study mentions that security strategies have been developed in many domains and, therefore, may possibly be

applicable in the improvement of safety strategies for the road (Hughes et al., 2015). Being that systems theory has been applied to various transport safety domains but never in a comprehensive, strategic manner for road safety, the scholars thought it important to provide this perspective to enhance knowledge in this field (Hughes et al., 2015). The scholars provide several studies that discussed different models, but none were of the nature presented in their study. The conclusion drawn from their study was that applications of safety models from the various domains could and should be used in road safety strategies (Hughes et al., 2015). Methods based on systems theory deliver a more comprehensive understanding of a broader range of components along with their interaction to affect a desired outcome (Hughes et al., 2015).

Systems of systems engineering. Keating, Katina, Bradley, and Pyne (2016) used GST to provide a strong foundation for developing system of systems engineering (SoSE). Systems-of-systems is defined as a condition where independent systems work together to achieve goals that are unable to be reached by the systems individually (Axelsson, 2019). Their study referred to the axioms and principles mentioned earlier in this study, along with others not mentioned, to provide implications for SoSE (Keating et al., 2016). There were no past studies laid out like in the other studies presented, but the scholars did cite a study that was used to validate statements made in this study. A table of attributes and orientations were presented as a summary of key distinctions, along with a diagram depicting the contributions of systems theory to SoSE (Keating et al., 2016). Their study concluded that GST could further develop the methods, processes, tools, and techniques of SoSE if it is considered in practice as GST grounds SoSE by providing a reference framework (Keating et al., 2016).

Leadership in education. Shaked and Schechter (2018) used GST to examine the development of school leadership among principals at various career stages. It was important to

include their study as it deals with the scholastic environment and how GST can be used to inform studies in this field. Being that this study looked at data custodians at the university level, including their study to provide an example for application seemed fitting. The scholars presented a series of previous studies that addressed this topic, but still found a gap in literature that sparked the development of their study (Shaked & Schechter, 2018). The scholars used interviews, focus groups and observations to gather data which was presented in the study using tabular form. This qualitative study concluded that the practice of developing systems thinking in school leaders occurs over several stages and is similar to structures described by other models (Shaked & Schechter, 2018). The scholars were able to further deduce that systems thinking, although not equally applicable, was appropriate with respect to features and context of the specified developmental stage each school leader was a part of at a given time (Shaked & Schechter, 2018).

Information Security

InfoSec is a primary concern for many corporations. The primary purpose of InfoSec is to provide protection of information and maintain that same information's confidentiality, integrity, and availability (Fazlida & Said, 2015). Confidentiality is preserved when information remains private, integrity is preserved when the information is dependable, constant, and correct, while availability is preserved when the information is always available (Alqahtani, 2017). An information security strategy is a plan that assimilates corporations' information security actions, goals, and policies into one cohesive unit (Horne, Maynard, & Ahmad, 2017). To properly implement an information security strategy, corporations must have the support of leadership responsible for development of said strategies (Montesdioca & Maçada, 2015). The following information elaborated on InfoSec management, InfoSec compliance and how universities handle

InfoSec. InfoSec management is composed of development strategies, actual implementation, maintenance of the implemented strategy and addressing the human factor using SETA.

Information security management. While reviewing the literature, InfoSec management seemed to consist of several components including initial development of Information security strategies and policies, implementation of those vetted operations, maintenance of the implemented operations and properly informing the managers and users of the operations. InfoSec is mainly supported by the development of ISPs, or information security policies, which guides employees by providing them explicit instructions with terms and conditions to follow to aid in information security (Alqahtani, 2017). It is said that if the organization's ISP is fragile, there could be a lack of protection of the organization's information (Alqahtani, 2017). To properly develop an ISP, there are several factors to focus on to make the policy comprehensive including password management, email/internet use, social media use, mobile computing, and information handling (Alqahtani, 2017). Each of these elements are used to evaluate an ISP in some institutions (Alqahtani, 2017). Each category is broken down in the ISP to make the document comprehensive.

Once the ISP is developed, it needs to be implemented into the organization. Implementation, when the ISP is disseminated to the whole organization (Flowerday & Tuyikeze, 2016), requires that all departments within an organization are involved and committed to adhering to the ISP (Fazlida & Said, 2015). As mentioned before, a weak ISP can lead to information disaster and an ISP is weakened when all parties do not properly follow the implemented ISP. There are several ways in which InfoSec requirements, policies and strategies can be implemented (Olifer, Goranin, Kaceniauskas, & Cenys, 2017). One method is to start with implementation of organizational controls (i.e., an ISP) and then move to deploying complex

technical solutions (Olifer et al., 2017). Other options provided were to (a) concentrate on main components (i.e., security management, communication security, access of information systems and secure InfoSec development), (b) focus on governance, operational and technical management, and (c) beginning with network security and ending with cloud security (Olifer et al., 2017).

There are a few issues in relation to implementation that must be addressed. One of the issues with implementation is cost being that cost assessment is complicated due to lack of controlled cost methods and problems with security solutions due to uncertainties (Olifer et al., 2017). InfoSec costs can be divided into two categories: Recurring costs, or costs applied annually for maintenance, and one-off costs, or costs applied in the infant stages of planning, design, and implementation (Olifer et al., 2017). Table 1 gives examples of InfoSec implementation cost examples.

Table 1

Information Security Implementation Costs

Description			
One-off costs		Recurring costs	
License	Licensing cost of tool or product. Only applied to vendor-based solutions.	Support	Support cost from the vendor. With some licensing schemes, a yearly fee has to be paid as well.
Policies	Policies and plans developed by to ensure organization information security requirements implementation and maintenance.	Administration	Costs for updaiting and configuring the solution. Reflecting changes in the business in the policies. User support (help desk).
Hardware	Hardware procurement, installation and configuration.	Monitoring	Monitoring the system.
Implementation	The full process of implementing the security measure. Usually this has impact on the infrastructure and the organization. The implementation of the security measure often is phased and can require a long term.	Auditing	Audits and tests performed to ensure the correct implementation and workings of the system.
Embedding	The embedding of the implementation in the organization. Employees are needed to be hired or get training. Other employes might also need training or at least be notified og the changes.		

Note. Adapted from "Controls-based approach for evaluation of information security standards implementation costs," by D. Olifer, N. Goranin, A. Kaceniauskas, & A. Cenys, 2017, *Technological and Economic Development of Economy, 23*(1), p. 200. Copyright 2017 by Taylor & Francis Ltd. Adapted with permission (see Appendix C).

Another issue with implementation is responsibility. Companies have trouble identifying which department is responsible for implementing a developed ISP (Fazlida & Said, 2015). Some corporations allow the responsibility to rest completely on technical managers and upper management, namely Directors, pay little attention to the process (Fazlida & Said, 2015). There is also the issue with relying primarily on technical solutions which makes a corporation rely too

heavily on technical controls, meaning more responsibility for the technical staff (Fazlida & Said, 2015; Sohou & Holtkamp, 2018). On the opposite end of the technological spectrum, there is also issue with non-technical aspects of implementation such as awareness and compliance, which was examined next (Fazlida & Said, 2015).

Flowerday and Tuyikeze (2016) conducted a study that indicated that the role of stakeholders and SETA were among the variables they deemed important for proper policy implementation. InfoSec customarily has been reliant on insiders, or employees, making proper security decisions (Thompson, 2013). This brings up the final tenant of InfoSec maintenance which is adequate education, training, and awareness of security protocols. Humans are one of the largest primary concerns when referencing information security as they have been pinpointed as a weak link, thus making an ISP and a SETA program within an organization imperative (Bauer, Bernroider, & Chudzikowski, 2017; Soomro, Shah, & Ahmed, 2016). It is projected that between 50% and 90% of security breaches are a result of human error in some fashion (Budzak, 2016). Universities do have IT divisions and many of these institutions offer measures to protect IT resource users, but there are some instances when choices made by direct users, like students, have significant security risk implications (Ndiege & Okello, 2018). Fortunately, there is an increase in the awareness of how important it is for humans to make proper decisions regarding information system safety (Ben-Asher & Gonzalez, 2015).

Implementation of an ISP could be rendered ineffective without proper SETA since education, training and awareness inform employees how to best protect the data within the organization (Soomro et al., 2016). Education gives corporations an idea of what the user knows, training provides the proper skills for the user, and awareness captures the users' attention (Furman, Theofanos, Choong, & Stanton, 2012). Studies show that InfoSec awareness plays a

critical role in risk mitigation linked to employee behavior within the organization (Safa, von Solms, & Furnell, 2016). Education and awareness make up the foundation of a SETA program, but to truly modify users' behavior, training is required (Furman et al., 2012). A campaign is another way of shaping training and awareness as it is constant and regular interaction with information security strategies (Budzak, 2016). As addressed earlier, cost is one of the impeding elements of proper implementation, thus making it a hindrance in maintenance. An ISP and a SETA program are both relatively low in cost but high in reward when applied and followed intently (Han et al., 2017). If a user views an ISP as unnecessary, they either attempt to circumvent or altogether ignore the policy. SETA, in its entirety, assisted with InfoSec compliance by raising employee awareness to their responsibilities and the policy's importance (Han et al., 2017; Reece & Stahl, 2015).

Information security compliance. To properly implement an information security strategy, corporations must have the support of leadership responsible for the development of said strategies (Montesdioca & Maçada, 2015). Studies show that there is a significant relationship between support of leadership and ISP compliance (Flowerday & Tuyikeze, 2016). To improve compliance, managers can implement InfoSec awareness programs, as mentioned previously (Bauer et al., 2017). Compliance behavior is defined as actions that do not go against an organization's ISP (Humaidi & Balakrishnan, 2018). Proper InfoSec conduct lessens the risk of a data breach in organizations (Safa et al., 2016). InfoSec compliance allows organizations to audit practices and determine if the organization is adhering to defined controls (Choi, Martins, & Bernik, 2018). Users circumventing compliance with an ISP has been identified as a serious InfoSec threat (Hovav & Putri, 2016).

Studies show that when employees are more devoted to their organization, they are less likely to attempt to circumvent an implemented policy (Safa et al., 2016). Compliance with ISPs can have a direct effect on the success or failure of information security strategies and ISPs; therefore, it is important that organizations endorse positive compliance and introduce penalties for non-compliance as positive compliance behavior can minimize security incidents and increase ISP effectiveness (Humaidi & Balakrishnan, 2018; Parsons et al., 2015). Penalties for non-compliance should be severe enough to dissuade users' from not following the set ISP in place (Alshare, Lane, & Lane, 2018). Creating a positive security culture and normalizing compliance by working it into the employees' everyday routine assists employees with accepting InfoSec requirements (Parsons et al., 2015).

For decades, researchers have examined why users behave in an insecure manner, even when they are aware of penalties that come with violating implemented ISPs (Moody, Siponen, & Pahnila, 2018). There are studies that indicate that compliance research is still developing which is why there is no comprehensive framework tailored to InfoSec management within different organizations (Chen, Wu, Chen, & Teng, 2018). The next section looks at some of these same factors within the university.

Information security in universities. Guaranteeing InfoSec within an information system requires looking at the entire situation and emphasizing the components of infrastructure, management, and application of security policies (Yilmaz & Yalman, 2016). A university can ease the life of its students and its faculty and staff by increasing the use of information systems (Yilmaz & Yalman, 2016). In that same point, with the increase of information system usage comes the increased need for proper InfoSec and a higher level of security precautions within the institution (Yilmaz & Yalman, 2016). With a more open academic environment and elevated

network connectivity, cyber-attacks are happening more often at educational institutions (Misenheimer, 2016). Over a 7-year period from 2005-2012, educational institutions experienced more reported InfoSec issues than any other industry (Misenheimer, 2016). Due to increased information system threats and attacks, it was extremely important to develop comprehensive security programs with the IT departments (Misenheimer, 2016).

Even with these statistics, there are few bodies of work that address InfoSec and data breaches in academic institutions. The gap in literature section addresses this issue further. Despite the lack of literature addressing university ISPs, security of university information assets should be a very high priority (Doherty, Anastasakis, & Fulford, 2009). Doherty et al. (2009) conducted research that revealed of their 122-university data sample, only 61 had current ISPs that were readily accessible online. Examining the policies was a way for the researchers to get a better understanding of the way universities looked at ISPs. In the wide variety of focuses, some of the policies focused on physical security while others focused on the confidentiality, integrity, and availability of data (Doherty et al., 2009). Identity theft, data exposure, and data breaches have been increasing and so has the costs associated with those crimes (Misenheimer, 2016). The next section of this review addresses these data breaches, corporation's data breach regulations, the process for litigation after a data breach, the financial impact of a breach, as well as how breaches are handled specifically within the university.

Data Breaches

A data breach is defined as a security incident that results in the accidental or unlawful loss, alteration, disclosure, or access to protected processed data (Schatz & Bashroush., 2016). Data breaches occur when an intruder can gather and use information for any reason whatsoever (Lorio, 2017). As mentioned before, data breaches have been occurring for years and they are

only increasing in frequency. All industries have been affected and there are no particular type of data being targeted. One of the largest identified types of data that is being obtained during a data breach is PII. PII refers to information that can be used to trace or completely identify a person (O'Neill et al., 2016). PII can be something that identifies the person (i.e., name.), contact information for the person (i.e., phone number) location information, and even account login credentials (O'Neill et al., 2016).

Studies show that the financial and reputational impact that a data breach has on corporations can be drastically reduced by the organization doing something about the breach prior to it taking place (Densham, 2015). Corporations can take a proactive approach to data breaches by following three (3) strategies: response in depth, 360-degree security, and the avocado and the coconut (Densham, 2015). Response in depth, which is best executed within an organization that already has implemented and adopted a comprehensive security strategy, is in place when an organization has a standard approach to gathering alerts, determining the necessary actions and responding effectively to the alerts (Densham, 2015). This strategy consists of the following steps: (a) detect, (b) aggregate, (c) analyze, (d) identify, (e) respond, and (f) improve (Densham, 2015). What is known as 360-degree security is in place when an organization follows a process that includes improvement, governance, proactive monitoring, and a response mechanism (Densham, 2015). This strategy focuses on security assurance and making sure that all actors in a network are protected against presented threats (Densham, 2015). Finally, the avocado and the coconut is a philosophy that describes the approach that should be taken to protect data within an organization. This strategy states that organizations should switch to an avocado approach, which allows data to pass freely while hardening the core where most valued data is stored, from the traditional coconut approach, which hardens the perimeter to present a layer of safety and security (Densham, 2015).

There are several strategies that can be used for protecting data as the above list is not all inclusive. System hardening is a defensive strategy that has various security measures applied at different layers of a system (Ibor & Obidinnu, 2015). With this strategy in place, an intruder must defeat each layer to compromise the data. Figure 2 below demonstrates a system hardening architecture that allows safer access to vital business data. Figure 3 below shows the system hardening architecture for the host level, which is included here to show that hardening security policies, is a necessary component in protecting data.

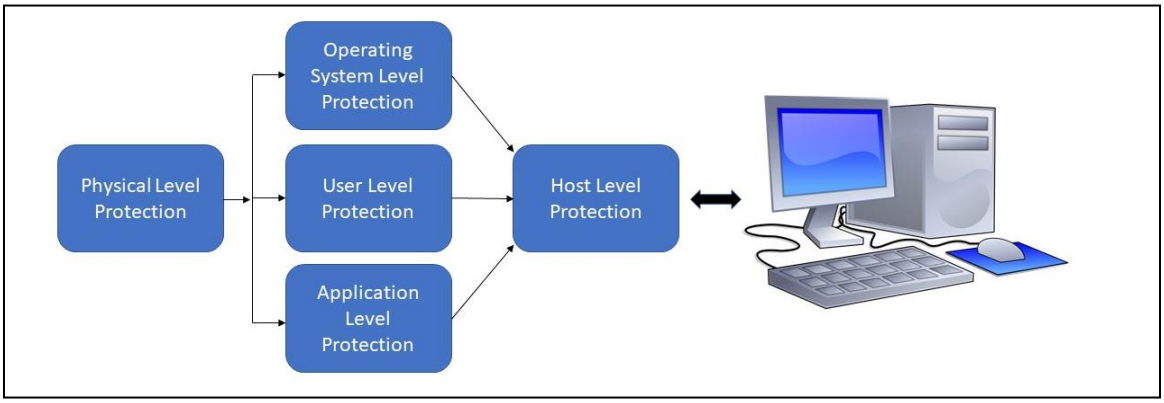


Figure 2. Layout for a system hardening architecture. Adapted from "System hardening architecture for safer access to critical business data" by A. E. Ibor & J.N. Obidinnu, 2015, *Nigerian Journal of Technology*, *34*(4), p.790. Copyright 2015 by Faculty of Engineering. Adapted with permission (see Appendix C).

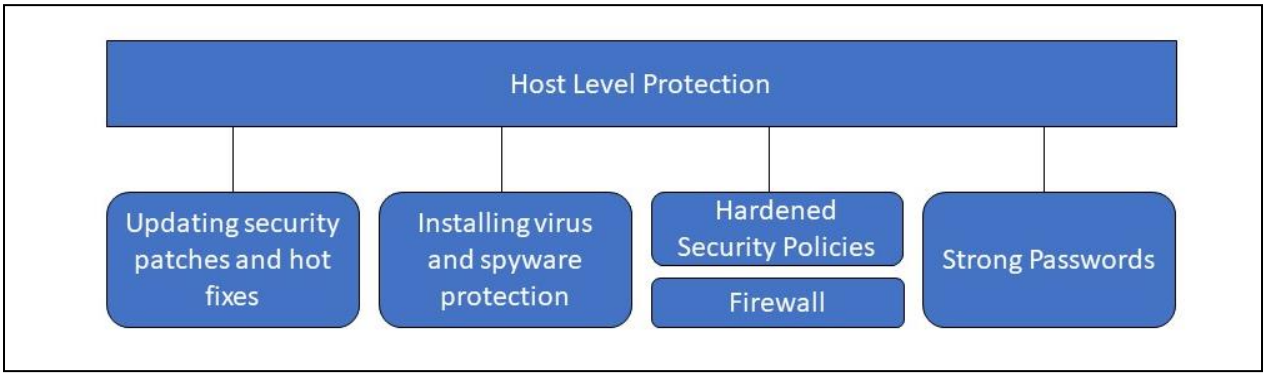


Figure 3. Layout for a system hardening architecture with host level protection. Adapted from "System hardening architecture for safer access to critical business data" by A. E. Ibor & J.N.

Obidinnu, 2015, *Nigerian Journal of Technology*, *34*(4), p.790. Copyright 2015 by Faculty of Engineering. Adapted with permission (see Appendix C).

System hardening, along with the other strategies, can be beneficial to protecting data within any corporation. Implementing said strategies require taking a further look at the regulations surrounding privacy and the other interrelated components.

Data breach regulations. Data is collected regularly from both public and private organizations and in doing so, these organizations must protect the collected personal data from unauthorized dissemination (Prakash & Singaravel, 2015). Privacy, or restricted access to a person and the associated information, is a person's right (Prakash & Singaravel, 2015). Data mining is a technique that is used to examine information from collections, which is executed by gathering information from data owners and then publishing that mined information to data recipients (public, researcher, etc.) for further review (Prakash & Singaravel, 2015). In this process, there are five phases that have been identified to address privacy of data that include: categorizing data as centralized or distributed, modifying data using approaches such as perturbation, aggregation, or noise addition, introducing data algorithms, hiding data that is considered private and can link back to the original data, and privacy preservation which include approaches such as data distortion and anonymization (Prakash & Singaravel, 2015). Some of the data presented in these data mining techniques belong to students and must remain private based on several regulations set up specifically for this population.

In 2014, California introduced the Student Online Personal Information Protection Act to safeguard student information and to make sure that the data remains the property of the school or district to which the student belongs (Varella, 2016). Where the Family Educational Rights and Privacy Act (FERPA) falls short, the Student Online Personal Information Protection Act picks up. FERPA regulations put parameters on the sharing of PII with third parties, stating that the

only way PII can be released without prior consent is when the party is directly affiliated with the institution and when the person is a school official that has a legitimate education interest in the information (Varella, 2016). FERPA, created in 1974, addresses protecting student information, but did not address the component relating to protecting student information in the cloud (Varella, 2016). Schools are increasing the amount of information that they are storing in the cloud, so it is important to introduce precautionary measures to protect this same data. Research indicated that, of the respondents in a national study, 95% use at least one type of cloud technology to process student data (Varella, 2016) Another national study indicated that the percent of cloud usage went from 27% in 2011 to 42% in 2012(Varella, 2016).

HIPAA, or Health Insurance Portability and Accountability Act, and the Federal Information Security Management Act are also sources of cyber security enforcement (Diaz, Anderson, Wolak, & Opderbeck, 2017). HIPAA requires the privacy and protection of protected health information on any channel of transmission while the Federal Information Security Management Act requires that a program to provide InfoSec be developed and implemented for all information systems throughout its entire agency (Diaz et al., 2017). HIPAA, FERPA, the Federal Information Security Management Act, and the Student Online Personal Information Protection Act all have fiduciary regulations and could prevent some entities from obtaining, or keeping, contracts or grants (Diaz et al., 2017). Violations of any of these regulations, related regulations, or a mishap in the actual protection and privacy of any data, could lead to litigation.

Data breach litigation. When data breaches occur, there are generally damages done whether they come in the form of financial set back to the individual that had an attacker use the information breached against them or if it is in the form of reputation damage to the company that allowed the data to be breached. Most corporations, by state law, are required to notify customers

that could have potentially been affected by a data breach. There are times where the customers decide to bring a class action lawsuit against the company that notified them of the breach indicating that the company was negligent and in breach of contract (Cease, 2014; Lorio, 2017). There are several issues that can arise after the lawsuit has commenced: (a) a standing concern, (b) choice-of-law concern and (c) class certification (Cease, 2014; Lorio, 2017).

A case or controversy allows a customer to sue a company, but there are three constitutionally mandated parameters of standing that include an actual or imminent injury, the injury must be traceable to the company's actions and a satisfactory decision will amend the injury (Cease, 2014; Opderbeck, 2015). A customer would have the most issues with meeting the injury requirement, especially when the information obtained in a breach was not used to make any purchases (Cease, 2014). Choice-of-law concern comes into play when there are several states involved in the suit since the federal court of each state is going to act according to its individual state legislation (Cease, 2014). The final issue that can arise is class certification which consists of two groups of mandates that must be met before a suit can meet the proper requirements.

The mandates from the first group consists of numerosity, where the class is so large that the number of affected individuals is impracticable, commonality, where there lie questions of law that are common among the class, typicality, where the claims of the affected must be typical of claims within the class, and adequacy, where the affected individuals will adequately protect the interest of the class (Cease, 2014). The mandates from the second group include questions of law that are common among the class must outweigh questions affecting the individual, variations in state laws are agreed upon by all presiding to enact one ruling in consensus, and that the class action suit is the only way to come to a fair and efficient resolution (Cease, 2014).

There is a lot to consider legally after a data breach has occurred. More developments in data breach litigation are occurring after the Clapper v. Amnesty International case where the metadata collection activities of the National Security Agency were challenged (Lorio, 2017; Opderbeck, 2015). Although many of the cases presented to the courts will be dismissed for not meeting the mandates above, companies can expect to see a continued rise in consumer class action suits after notifying the affected (Opderbeck, 2015). Many of the cases will be dismissed since many jurisdictions opt for the more stringent approach to the above doctrines while some others have adopted the liberal approach (Lorio, 2017). There have been suggestions made to Congress to adopt a comprehensive statute that regulates data breaches so that the victims of these breaches can receive a satisfactory remedy.

Data breach financial impact. Data breaches are becoming more common and the affected organizations tend to experience substantial financial cost, which usually includes rectifying the issue, addressing legal responsibilities, brand reimaging and repositioning market shares (Gwebu, Wang, & Wang, 2018). Researchers looking to provide more substantial numerical information on the financial impact associated with data breaches found that breaches have a negative impact on shareholder wealth (Gwebu et al., 2018). The Ponemon Institute completed a study on the cost of data breaches and found that there was a significantly higher financial impact when the data breach was categorized as a malicious attack (Schatz & Bashroush, 2016). Attacks are becoming much more damaging even with increased efforts to prevent security breaches (Schatz & Bashroush, 2016). In 2013, Target retailer suffered from a data breach that affected 70 million customers and after lawsuits, fines, revenue loss and response to the breach, the cost of the incident was over $450 million (Hemphill & Longstreet, 2016). In 2014, Home Depot suffered from a data breach that affected 56 million customers that cost the

company $62 million (Hemphill & Longstreet, 2016). In 2014, surveys found that over 100,000 security incidents were reported by 70 corporations from various industries representing 61 countries that involved 700 million affected records which resulted in an estimated financial loss of $400 million (Pawlowski & Yoonhyuk, 2015). The Ponemon Institute took an independent survey and found that from 2010 to 2014, the average data breach cost companies $4.2 million with 2014 alone averaging $8.6 million, which is 105 percent higher than the 5-year total average (Hemphill & Longstreet, 2016). The listed averages came from the retail sector alone, meaning that these numbers could be higher if other industries such as healthcare, government and education were included. Even with these numbers, students were surveyed and reported that they believed that it was unlikely that they would suffer a security incident within the year to come that would result in financial loss (Pawlowski & Yoonhyuk, 2015).

Properly managing the response to a breach can mitigate negative impact on reputation as well as reduce the cost of a response (Brown, 2016). One way to mitigate the financial impact is to establish financial regulations. Understanding that there is a need to protect customer data, and mitigate financial losses, major credit card brands developed a council to establish retail regulations (Hemphill & Longstreet, 2016). The Payment Card Industry Data Security Standard, or PCI DSS, is managed by the Payment Card Industry Security Standards Council, or PCI SSC, which was founded in 2006 with primary goal of protecting customer's PII (Hemphill & Longstreet, 2016). PCI DSS lists 12 requirements for merchants to comply with the 12th requirement being that a merchant must maintain an ISP (Hemphill & Longstreet, 2016). Another way to mitigate cost is to establish business continuity management. An actual business continuity management plan could potentially reduce cost by $7.10 per record (Brown, 2016). This means that Target suffered a loss that affected 70 million customers with an associated cost

of $450 million, which could have been reduced by $4,970,000 if each customer represents one record and Target had a business continuity management plan.

Data breaches in universities. The U.S. Department of Education recognizes that higher education is susceptible to data breaches because colleges and universities have access to much of the same information that banks have, but are much easier to access (Diaz et al., 2017). The editor-in-chief of Computers and Security, Dr. Eugene Schultz, stated that universities are among the least secure facilities in the universe in relation to computers (Ncube & Garrison, 2010). In 2006, Oklahoma State University concluded that the number one reason for breaches in data via account access was the strength of the password (Farcasin & Chan-tin, 2015). The university enacted a password policy to assist with the potential issue, even though the study revealed that many users attempted to circumvent the password policy, thus reverting back to the idea that the human factor, not the password or surrounding policy, is the root of the problem (Farcasin & Chan-tin, 2015). Another part of the human factor at the college and university level are university professors. Many professors do not have the InfoSec knowledge that they need to properly protect student data as they are specialists in their field, but generalists in InfoSec (Mäntykangas, 2018).

Over the 9 year stretch from 2005 to 2014, educational institutions were the victim of data breaches over 700 times (Beaudin, 2015). From 2005 to 2009, 290 incidents occurred resulting in almost 11,000,000 records being breached with 50% of the data categorized as stolen and 43% categorized as hacked (Ncube & Garrison, 2010). These data breach statistics were attributed to the amount of information that universities have access to, as well as their inferior security measures (Beaudin, 2015). Many colleges and universities are not even considering InfoSec a vital issue much less setting up a security plan to address any other InfoSec issues,

making them much more susceptible to cyber security issues such as malware infections (Beaudin, 2015). A misappropriation of information can occur because of hacking, theft, a malicious insider, improper disposal, as well as accidental exposure (Beaudin, 2015). Data that could be obtained from a breach at a college or university includes medical information recorded from on-campus medical centers, personal information recorded from admissions, and financial information recorded from the bursar (Beaudin, 2015).

Universities and colleges are meant to protect data from breaches, not just to provide access to users (Joshi & Singh, 2017). There is absolutely a need to improve the security of the data available to the university or college, which requires risk identification, vulnerability assessment and continuous monitoring (Joshi & Singh, 2017). There is still much work to be done to get to the point where the information is adequately protected, and with a large gap in literature on the topic, there is a lot of opportunity to study this topic and increase the breadth of knowledge on this topic.

Gap in the Literature

With all the studies that have been conducted revolving around InfoSec, there is still a significant gap in literature. Many of the studies do not contribute to the understanding of data breach risks, nor do they assist with preparing for future data breaches (Sen & Borle, 2015). Research is necessary to explore the factors related to the risks of a data breach (Sen & Borle, 2015). Knowing how frequently data breaches occur, as well as their financial impact and their increasing trends, serious improvements need to be made in understanding the risk of a data breach (Sen & Borle, 2015). Presently, literature referencing InfoSec mainly focuses on the financial impact of publicly releasing information on InfoSec breaches (Sen & Borle, 2015). The literature also lacks an agreed upon typology, which is required to summarize and predict

research (Zhu & Janczewski, 2015). This creates further issues, resulting in dozens of theories and methods being used making it even more difficult to establish a single topology (Zhu & Janczewski, 2015).

There is also a gap in literature when examining the structure, scope, and content of an ISP (Doherty et al., 2009). Current literature lacks contribution and consensus while rarely addressing the specific issues that should be addressed by the ISP (Doherty et al., 2009). A gap exists when address approaches to formulating an ISP, which is said to be a result of not fully comprehending the structure of a comprehensive policy and the scope that the policy should have (Doherty et al., 2009). Little information has been published on how to apply a newly fashioned ISP, thus rendering other information provide in respect to the policy unsuitable for consumption (Doherty et al., 2009). I conducted this research to fill the gap in the literature by analytically investigating the structure and content of comprehensive university ISPs instead of just generalizing about what the policy should include.

Transition and Summary

The purpose of this study was to examine the information security strategies that university data custodians use to protect PII collected from staff, students, and other stakeholders. This section introduced the issue of data breaches at the college and university level. This section also provided a summary of the nature of the study, presented assumptions, limitation, and delimitations, as well as provided more context for terms to be used within this study. The review of literature contributed more information on GST, data breaches, InfoSec, and the gap in literature for a better understanding of all concepts.

Section 2 provides information pertaining to the research method and design selected for this study. It also contains information surrounding the role of the researcher, participants,

population, and sampling as well as ethical concepts. Data collection, organization and analysis techniques are examined in Section 2 as well.

Section 3 contains the results of the study based on the data collected from the research participants. It will also discuss the applicability of the findings with respect to the professional practice of IT. This information will be followed by implications for social change and recommendations for action and further research. Researcher reflections will be followed by a conclusion of the document.

Section 2: The Project

In this section of the study, I discuss the role that the researcher plays along with the means of managing the participants. The research method and design chosen for this qualitative study will be elaborated on to further expand on the information provided in Section 1. Next, I will explore the population and sampling methods, followed by a listing of ethical considerations that were taken during this study. The data collection, organization, and analysis techniques selected for this study will be discussed and the section will conclude with an explanation of how this study will achieve reliability and validity.

Purpose Statement

The purpose of this qualitative case study was to examine the information security strategies that university data custodians use to protect PII collected from staff, students, and other stakeholders. The original targeted population consisted of data custodians from 30 universities in North Carolina and South Carolina who have implemented security strategies. The implication for positive social change is that improved security strategies have the potential to minimize the chances of identity theft or any other negative effects of a data breach involving Carolinians affiliated with universities.

Role of the Researcher

The role of the researcher in the data collection process was to develop a management and sharing plan for data according to ethical obligations, policies, and standards (Chauvette, Schick-Makaroff, & Molzahn, 2019). The researcher should be closely entrenched into the research location, the study participants, and the data being collected (Yates & Leggett, 2016). In this study, data were collected using semistructured interviews. I acted as the data collection instrument by recording the interviews for transcription and coding after completion. For this

study, there was no direct relationship between the participants and me. My relationship with the topic stemmed from the fact that I was a university student or affiliated with a university for 19 years. I attended, graduated from, and applied to 17 colleges and universities since 2000. Of those 17 colleges and universities, eight have been subjected to a data breach since 2005 (Privacy Rights Clearinghouse, 2018). During my 3.5 years in an undergraduate program at Purdue University, there were six breaches publicly announced (Privacy Rights Clearinghouse, 2018). This means that the likelihood of my PII being at risk was substantial showing why this topic is important to me. I have resided in North Carolina, South Carolina, and I have applied to North Carolina Agricultural & Technical University, one of the universities in the targeted population area. This was the only relationship that I had with the location.

The role of the researcher when referencing ethics is to identify any risks present and take exceptional safety measures to protect subjects, especially those subjects in populations that could be considered vulnerable (Call-Cummings, Dennis, & Martinez, 2019). To make sure this study aligned with ethical obligations, policies, and standards, I used the Belmont Report for guidance. The Belmont Report lists the three basic ethical principles as respect of persons, beneficence, and justice (U.S. Department of Health and Human Services, 1979). Respect for persons incorporates the convictions of treating individuals as self-governing agents and to protect those who have a reduced aptitude to self-govern, beneficence can be demarcated by a researcher maximizing benefits and minimizing harms, and the principle of justice states that equals should be treated equally (U.S. Department of Health and Human Services, 1979). Adhering to the listed convictions generated proper alignment between me, ethical obligations, and ethical considerations.

Qualitative studies generally use focus groups or interviews to collect data (Guest, Namey, Taylor, Eley, & McKenna, 2017). The rationale for using semistructured interviews in this study was that interviews are a cost-effective way to get the greatest depth and detail from study participants (Guest et al., 2017). With semistructured interviews, I was able to view matters brought up by the participants because the list of questions for the interview only contain a few predetermined questions (McGrath, Palmgren, & Liljedahl, 2018). To confirm thoroughness in a research study, bias must be mitigated (Squires & Dorsen, 2018). Bias occurs when the researcher attempts to influence the thoughts and opinions of participants in a research study (Squires & Dorsen, 2018). Bias was mitigated in this study by avoiding leading questions during the interview process, only providing the data retrieved from the study regardless of how it supports the claims in this study, and ensuring that the study could be reproduced by another scholar. Mitigating bias is much easier when the researcher understands that bias is present in the research, both from the researcher and the participants (Fusch, Fusch, & Ness, 2018). To view the data from a personal lens, the researcher must realize that bias is present in the data both intentionally and unintentionally (Fusch et al., 2018). If a researcher can recognize their personal view and its presence, that researcher is then better equipped to interpret the views and behaviors of others (Fusch et al., 2018).

Participants

For a person to be considered for this study, the following criteria had to be met: (a) must hold the title of data custodian or a title with similar responsibility and (b) must be responsible for a college or university located in North Carolina or South Carolina. A data custodian is an individual who collects, manages, and stores data collected for various reasons and would be held accountable for data distribution (Smith et al., 2015). With a more open academic environment

and elevated network connectivity, cyberattacks are happening more often at educational institutions (Misenheimer, 2016). Qualitative study participants are selected based on their relevance; university data custodians were the participants for this study because data custodians are responsible for managing data at colleges and universities (Clark & McLean, 2018). Qualitative sample sizes are usually small because the research concentrates on the quality of the information provided, thus providing a basis for choosing North Carolina or South Carolina universities instead of several universities from every state (Quick & Hall, 2015).

Gaining access and selecting participants are just two of the conditions necessary to foster a quality interview (Castillo-Montoya, 2016). Participants in a qualitative study are chosen deliberately and there needs to be a strategy to gain access to them (Moser & Korstjens, 2018). The strategy to gain access to the personnel needed for this study began with Internet searches for colleges and universities in North and South Carolina. I developed a list that included the name of the university and the phone number to the IT department along with the names and email address of personnel who were identified as data custodians at the university. The amount of information that a researcher reveals to participants can directly influence a researcher's ability to gain access to possible participants, establish a solid relationship, and collect data (Gesch-Karamanlidis, 2015). With that in mind, the data custodians were then contacted via an email that divulged information about who I am, explaining the study, as well as the impact the study could have on the university's students, faculty, staff, and other stakeholders. The email also included my contact information and instructions for the data custodian if they wished to participate.

Establishing rapport by way of indicating that the participants' time is appreciated is the responsibility of the researcher at the initial point of contact, whether by email, mobile chat, or phone call (Miller, 2017). Gaining trust and having the necessary skills to encourage participants

to speak about their experience are required when establishing a working relationship with participants (Herrmann, 2017). The strategy I used to establish a working relationship, or rapport, with the participants was to speak professionally via all communication channels, remain flexible and accommodating for meetings, show up or call early for scheduled meetings, and provide thank-you notes via mail to all participants. Because validating participants' experiences through normalization is standard for establishing a working relationship during qualitative interviews, this technique was used throughout the entire interaction with the participants (Wolgemuth et al., 2015).

Research Method and Design

Research Method

This qualitative study examined the information security strategies that university data custodians use to protect PII collected from staff, students, and other stakeholders. The qualitative methodology was chosen for this study because the qualitative method is used when something is not well defined and needs exploration, the problem is complex and requires description, the context of a problem calls for in-depth observation, there is a necessity to explain linkage, and when measurement is not particularly warranted (Yakhnich, 2016). Qualitative methodology is also used when trying to explain a phenomenon or a particular outcome (Clarke, Boyce-Gaudreau, Sanderson, & Baker, 2015). A qualitative approach was more suitable for this study because the goal of the study is to access the thoughts of data custodians regarding information security strategies to be able to develop a better understanding of how they protect collected PII (Sutton & Austin, 2015).

Quantitative research methodology uses an arduous and controlled strategy to precisely measure an occurrence (Rutberg & Bouikidis, 2018). It is used when trying to confirm a

hypothesis using statistical data to quantify how many people participate in a certain behavior (Sutton & Austin, 2015). This study did not set out to test a theory nor was it trying to confirm a hypothesis. Quantitative research is generally linked to a study that is deductive and objective where the research and design generates statistical data (Morgan, 2018). This research did not necessitate the use of statistical data as its main component (Inoue, Ghosh, Chatterjee, & Chakrabarti., 2015), which is another reason the qualitative methodology was used in this research.

Mixed methods research uses both qualitative and quantitative research elements to gather a better depth of understanding (Almalki, 2016). Mixed methods research also takes longer to complete due to the need to collect both qualitative and quantitative data, whether the data is collected concurrently or sequentially (Taguchi, 2018). Assimilating data from two different methods is a challenge (Wilkinson & Staley, 2019). Given this fundamental challenge along with the length of time that it takes to complete a mixed methods study, choosing exceptional data points from either predominate research method, in this case the qualitative method, was the better option.

Research Design

Case study, ethnographic, narrative research, and phenomenological designs were the viable options for this qualitative study. Case studies allow for reflection by relying on narratives, professional knowledge, and/or professional experiences and it is commonly recognized for is strength mainly due to its flexibility (Short et al., 2017). Scholars using the case study design seek to investigate a problem in its natural context with one or more cases (Shaw, 2013). The case study design was used in this study to examine information security strategies used by data custodians in its natural context at different universities. The goal of this research was to gather a

deeper understanding of the information security strategies, which was one of the primary reasons that case studies are used (Ali et al., 2018).

Ethnography is defined as the science of depicting a culture (Lanclos & Asher, 2016). Ethnography is best suited for providing great descriptions of people's experiences and answering the why and how about cultural practices (Lanclos & Asher, 2016). This study looked at the security strategies that were used to protect data, not at the social or cultural practices in universities or among data custodians. Ethnography is the study of beliefs and behaviors of small societies (Mohajan, 2018), which was not the target for this study. Although ethnography can be used to guide decisions to help improve services (Ramsden, 2016), it was not appropriate for this study based on the aforementioned reasons.

Narrative research provides individual stories for development (Lewis, 2015). Narrative research was not chosen as there are no stories to examine, only information security strategies. Scholars engage narrative research to gather stories and then converse about the meanings of the experiences within the stories (Gous, Eloff, & Moen, 2014). Narrative research is generally used to study educational practices and elaborate on how humans experience the world (Sato & Haegele, 2016). The concern in this study did not factor in how data custodians experience the world. Since the focus was on the security strategies, narrative research was not appropriate for this study.

Phenomenological studies investigate the lived experience of a given phenomenon (Percy et al., 2015). Phenomenological design, although considered at the primary stages of this study, was not chosen because the primary focus of this study was not the lived experience of a data custodian. A researcher, when using the phenomenological approach, is to accurately define the phenomenon absent any pre-assigned framework while staying true to the facts (Groenewald,

2004). The researcher also must use the approach to gather a deeper understanding of the topic of choice (Nottingham & Mazerolle, 2018). It is for these reasons that this approach was considered in the primary developmental stages; however, the case study approach deemed itself more appropriate as it is more flexible and relies on a wider variety of reflection areas.

When conducting qualitative research, the issue of reaching data saturation surfaces when interviewing participants (Fusch & Ness, 2015). Saturation is used as a measure for discontinuing data collection and analysis (Saunders et al., 2018). Data saturation is reached when there is sufficient data to reproduce a study, the capability to acquire additional information has been achieved, and when additional coding is no longer practical (Fusch & Ness, 2015). Data saturation was ensured in this study by exhausting all viable participants in the target area and verifying that all data points are thoroughly documented for future replication.

Population and Sampling

The original targeted population consisted of data custodians from 30 universities in North Carolina and South Carolina that have an implemented set of security strategies. The criteria required for each participant was a title of data custodian, or the responsibility similar to that of a data custodian, and responsibility for a college or university located in North Carolina or South Carolina. A data custodian is an individual or group of individuals that collect, manage, and store data collected for various reasons and would be held accountable for data distribution (Smith et al., 2015). It should be noted that the participants, or who was selected, would depend on the intentions of the research being conducted (Bolderston, 2012). As stated before, since qualitative study participants are selected based on their relevance, it was acceptable to use university data custodians as the participants for this study because data custodians are responsible for managing data at colleges and universities (Clark & McLean, 2018).

Sampling involves selecting participants that offer rich data regarding the topic of interest (Moser & Korstjens, 2018). There are several sampling methods that could be applied to this study; however, the sampling method that most directly applied is the criterion sampling method. Criterion sampling selects participants that meet pre-determined criteria of importance (Moser & Korstjens, 2018). To make sure that the participants are providing adequate data, they must meet certain criteria as stated previously in this document. A data custodian that has no knowledge of what a security strategy is, nor how it benefits their organization, may not be able to provide useful information for this study as it is an examination of security strategies. Other viable options included purposeful sampling, where the participants possess certain traits or qualities (Gentles, Charles, Ploeg, & McKibbon, 2015), and convenience sampling, where the participants are available and easy to contact (Koerber & McMichael, 2008). Purposeful sampling could lead to a large bias and skewing of data while convenience sampling could yield participants that are unable to adequately provide the information being solicited. For these reasons, the choice to use criterion sampling was solidified.

In a case study, the suggested sample size should be less than four or more than 15 cases (Gentles et al., 2015). Unlike quantitative studies, qualitative studies generally do not have a preset sample size (Kuper, Lingard, & Levinson, 2008). The appropriate number ultimately lies in the complexity of the topic and the depth of data being collected from sources (Gentles et al., 2015). Having up to 30 data sources with the knowledge to answer the questions needed for this study would suffice. An estimate of sample size is essential for development of the study, but it must be kept in mind that the appropriateness of the final sample size must be constantly evaluated during the research (Malterud, Siersma, & Guassora, 2016).

As mentioned before, saturation is used as a measure for discontinuing data collection and analysis (Saunders et al., 2018). Data saturation is reached when there is sufficient data to reproduce a study, the capability to acquire additional information has been achieved, and when additional coding is no longer practical (Fusch & Ness, 2015). Data saturation determines what the sample size of a study should be, and it differs depending on the study (Moser & Korstjens, 2018). For this study, data saturation was achieved by conducting interviews until the same information was being recorded. According to Saunders et al. (2018), this is a signal for the researcher that data saturation has been achieved and that it is time to analyze the data. Although the goal was to interview data custodians at 30 universities, when the interviews started to yield redundant information around the 15th interview, no more interviews commenced, and the data collected was analyzed.

Qualitative studies generally use focus groups or interviews as the data collection method in a study (Guest et al., 2017). This study used semistructured interviews as the data collection method. The rationale for using the semistructured interview style of data collection in this study was that interviews are a cost-effective way to get the greatest depth and detail from study participants (Guest et al., 2017). The interview setting for this study was virtually via various teleconference solutions and at a time chosen by the participant to make sure that they were comfortable (Dempsey, Dowling, Larkin, & Murphy, 2016). The locations were isolated, discreet, and allowed for an uninterrupted interview, meaning that all electronic devices were turned off along with anything else that could pose as a distraction (Bolderston, 2012). I also needed to be sure that the device being used to later transcript the interview, whether it was video or audio recording, was checked prior to the start of the interview. There was ample time allotted to secure materials such as batteries, lens cloths or anything else required. Due to school closings to thwart

the spread of COVID-19, the meeting locations were chosen independently, and no face-to-face interviews were held.

Ethical Research

Consent is defined as a negotiation of trust that requires continuous renegotiation (Orb, Eisenhauer, & Wynaden, 2001). In qualitative research, informed consent allows participants to exercise their right to willingly accept, or refuse, to contribute to a study (Orb et al., 2001). For this study, participants were given a participant consent form (Appendix A). The form stated that the participation was voluntary, withdrawal could occur at any time, and that the information obtained would be kept confidential. In research, it is ethically and lawfully problematic to ask any potential participant to waive their right to withdraw (Peter, 2015), thus procedures for withdrawal were informal, but required in writing for tracking purposes. This information was also made available on the participant consent form. It is ethically acceptable to provide small incentives for participation in research when the research comprises of low risk (Graham, Powell, & Taylor, 2015). As there were no incentives for participating, there was no mention of incentives on the form.

Ethical issues do not just concern individuals, but the institutions as well (Qamar, 2018). To assure that the protection of the participants is adequate, respect not only considered the individual sharing the information, but the institution of which the participant represented. No findings were falsified, distorted, exploited, nor criticized before, after, or during any stage of this research process. Respect for persons is the first principle of the Belmont report (Miracle, 2016) and it was upheld from the beginning to the end of the study.

Confidentiality is another concern during research, and it needs to be addressed during the recruitment, data collection, analysis, and dissemination of results phases of the study

(Petrova, Dewing, & Camilleri, 2016). Being sure to maintain the confidentiality of a participant may diminish the participants' exposure to any opportunity for negative actions or reactions from others (Lancaster, 2017). Data collected from each participant will be maintained in a secure place for 5 years to protect the confidentiality of the participants. The names and affiliated institutions of the participants were not used to share the data as each participant was represented via unique code identifiers I created. Another measure taken to ensure confidentiality on behalf of the participant was minimizing the disclosure of demographic information as suggested by Petrova et al. (2016).

Data Collection

Instruments

The data collection instrument used for a qualitative study could be a questionnaire, observation, or an interview (Limakrisna & Ali, 2016). Although I was the primary data collection instrument in this study, the additional data collection instrument that was used in this study was the semistructured interview. Semistructured interviews, generally oral in nature, are commonly used as the collection instrument in qualitative data (Percy et al., 2015). Semistructured interviews allow the research participants to express concern relating both to themselves as well as the topic at hand (Blagden & Perrin, 2018). This process allowed for collection of data in both an efficient and cost-effective manner all while keeping the collection stage of the research phase open and unobtrusive (O'Keeffe, Buytaert, Mijic, Brozović, & Sinha, 2016). This style of interview was also used in this study to build rapport with the participants and allow them to think about the research topic while speaking candidly and uninhibited (Blagden & Perrin, 2018). A structured interview was not chosen as it is mainly used to collect quantitative data (Dikko, 2016) and focus groups were not chosen due to the location of the

participants along with the understanding that the sum of the research participants' experiences did not offer more value to the research (Paradis, O'Brien, Nimmon, Bandiera, & Martimianakis, 2016).

Reliability is attained when the instrument of measurement consistently measures what it is supposed to without bias (Dikko, 2016). Validity is attained when the instrument of measurement adequately represents the measure that it was supposed to in relation to content, construct, and criterion (Dikko, 2016). Reliability and validity of the semistructured interview process were enhanced by using member checking. Member checking was used to authenticate and assess the credibility of the qualitative results I collected (Birt, Scott, Cavers, Campbell, & Walter, 2016). It provided a way for me to verify that the participant was being accurately represented by giving the participant a chance to confirm, or deny, that the information provided was accurate (Candela, 2019). It was used in this study to facilitate an ongoing validation of the data, themes and conclusions gathered from the individual participants (Hadi & Closs, 2016). Transcript review was done before and after member checking solely to gauge the number of changes made after member checking. The interview protocol used for this study can be found in Appendix A. The interview questions asked to the research participants can be found in Appendix B. A pilot test was conducted once the IRB approval number 01-09-20-0454602 was granted. The pilot study results indicated that two interview questions needed to be reformulated based on industry expert feedback. The questions were deemed to potentially be taken as intrusive by participants so, in turn, they were reformulated to render a general answer that would suffice for data collection.

Data Collection Technique

The data collection technique that was used to collect data was an interview. Interviews in a qualitative study are conducted by the researcher by asking participants questions via phone, online, or in person (Moser & Korstjens, 2018). Interviews are usually conducted in multiples of 10 (Saunders et al., 2018), so 30 interviews were the target if saturation had not been reached at 15. Interview questions for this study were semistructured in that there was a predetermined list of questions, but the participants were encouraged to reply to any of the questions in greater depth (Queirós, Faria, & Almeida, 2017). Each participant was asked the list of interview questions located in Appendix C via conference call technology (Zoom and FreeConferenceCall.com) to make sure that there was an audio transcription of the conversation. Due to the pandemic, because of COVID-19, this method was the only acceptable option to host the interview. Transcription is defined as the process in which entities externalize language in written text form (Alves et al., 2016). Each interview had the audio recorded for adequate transcription once all the interviews had been conducted. Administering audio recording for transcription, with the participants' consent, is vital as it allows for accurate transcription of the conversation later (Gill & Baillie, 2018). Qualitative interviews are transcribed prior to being analyzed to decrease the number of limitations linked to natural biases (Azevedo et al., 2017). The audio transcription for this study occurred using the free, open source software oTranscribe.

There are several advantages and disadvantages to using interviews as the data collection technique. One of the advantages to using interviewing, specifically semistructured interviewing, as the data collection technique was that it facilitates mutuality between the researcher and the research participant (Kallio, Pietilä, Johnson, & Kangasniemi, 2016). Another advantage to using semistructured interviewing as the data collection technique was that it permitted the chance for

information that was formerly unknown to surface (O'Keeffe et al., 2016). The ability to have some flexibility within the interview was another advantage to using semistructured interviewing as a data collection technique (Adhabi & Anozie, 2017). One of the disadvantages to using semistructured interviewing as the data collection technique was interviewer and interviewee bias (Young et al., 2018). Another disadvantage to using interviewing manifested in the type of interviewing that was used. This study originally was to use face-to-face and telephone interviews to interact with research participants. Face-to-face interviews can be costly and may require a great deal of time to complete (Adhabi & Anozie, 2017). Telephone interviews have a disadvantage since the interviewer and interviewee are unable to see one another (Gill & Baillie, 2018). Video teleconferencing was chosen to conduct the interviews due to the pandemic. This was a free option that allowed the participant and I to meet face-to-face without being in the same room.

A pilot study is demarcated as a trial run conducted in preparation of the actual full-scale study, mostly used to pretest a data collection instrument (Dikko, 2016). A pilot study is necessary because it allows for refinement of the data collection instrument as well as ensuring the attainment of research validity (Hayashi, Abib, & Hoppen, 2019). Pilot studies are also able to let a researcher estimate the amount of time that may be needed to complete the actual study (Kinchin, Ismail, & Edwards, 2018). Pilot testing cannot be conducted until IRB approval is obtained. This approval requires all parties involved to submit an IRB application requesting approval. Once that is complete, the pilot study, as well as the full-scale study, can commence. Any data collected prior to approval will not be recognized by the university.

Member checking is the continuous validation of data, analysis of research themes and other components collected from research participants (Hadi & Closs, 2016). In qualitative

studies, member checking is used to supplement the study's rigor and validity (Birt et al., 2016). With this study being qualitative, member checking was used to create trustworthiness in the research and mitigate any researcher bias that could surface (Candela, 2019).

Data Organization Techniques

Consistency is the first rule of data organization (Broman & Woo, 2018). Having a data organization technique from the beginning is important because it allows you to organize your data in a consistent manner early during the research, thus preventing time being spent later trying to shape the data (Broman & Woo, 2018). There are several data organization techniques that can be used in qualitative studies; however, for this study research logs and cataloging systems were used. Research logs can be used not only to organize data, but also to reflect on problems that can arise during the data collection phase of research (Annink, 2017). Research logs, also referred to as research diaries or journals, makes the research process visible and has been affirmed as an effective tool to organize the research process (Refaei, Kumar, & Harmony, 2015). Research logs also help to facilitate sentience of the researcher's principles, biases, and experiences (Burley, Cox, di Tommaso, & Molineux, 2018). Data collected from each participant will be maintained in a secure, virtual safe for 5 years to protect the confidentiality of the participants.

A cataloging system was also used in this study to organize data. A data cataloging system can offer the researcher a valuable roadmap of acquired data, making it simpler to locate, access, and understand collected data (Stillerman, Fredian, Greenwald, & Manduchi, 2016). The SUV model that was used to create the interview questions were also used to categorize the collected data. This model takes a systems-based approach and is derived from GST (Jokela et al., 2008). It consists of three levels and seven categories. The three levels are individual, technology, and organization. The seven categories are goal seeking, regulation, hierarchy and relations,

differentiation and entropy, transformation process, input, and outputs (Jokela et al., 2008). QDA Miner is a qualitative data analysis tool that is used to code textual data (Ropret, Aristovnik, & Kovač, 2018) and it was used in conjunction with the research logs to organize the collected research data. The free version, referred to as QDA Miner Lite, was used because the budget for this research did not include software purchasing.

Data Analysis Technique

Data analysis in a qualitative study refers to the method of turning information collected in the data collection phase into evidence-based elucidations that are clear and understandable (Ubit & Bartholomaeus, 2018). There are four types of triangulation data analysis processes that are applicable to case study research design which include: (a) multiple data sources, (b) multiple methodologies, (c) multiple theoretical schemes and (d) multiple researchers (Haydn, 2019). The appropriate triangulation data analysis process for this case study was multiple data sources as I collected data from two different states with an initial goal of 30 different colleges and universities. To be classified as the multiple data sources triangulation method, the researcher must be gathering information from different locations, time periods or perspectives (Natow, 2019). There are several advantages to using this triangulation method; however, the most prominent advantage is that data triangulation enhances the research's validity (Razmi-Farooji, Kropsu-Vehkaperä, Härkönen, & Haapasalo, 2019).

Manners, Kruger, & Saayman (2016) make mention of the six steps of data analysis that will be combined with Tesch's, 1990, eight steps for coding data (Akçayır, M. & Akçayır, G., 2017) to establish a logical and sequential process for the data analysis. The six steps of data analysis include: (a) categorize and compose the data, (b) read over all of the data, (c) begin coding analysis process, (d) generate descriptions, categories and themes during the coding

process, (e) propose the descriptions, categories and themes will be embodied in the qualitative account and (f) make an interpretation/explain the meaning of the data (Manners et al., 2016). Braun and Clarke, 2006, presented six steps almost identical, although less formal, to that of the steps mentioned by Manners, Kruger, & Saayman, further indicating that the steps provided are sound and reliable (Origlia Ikhilor et al., 2018). The eight data coding steps include: (a) get a sense of the entire subset of data, (b) choose a document and get an understanding of its underlying meaning, (c) develop major topics by repeating step two for several research participants, (d) create an initial coding scheme, (e) group the coding scheme into categories, (f) finalize the category abbreviations and organize them accordingly, (g) gather all associated data with a particular code in one location to begin analysis and (h) recode as needed (Akçayır, M. & Akçayır, G., 2017).

As mentioned before, QDA Miner is a qualitative data analysis tool that used to code textual data (Ropret et al., 2018) and the free version, referred to as QDA Miner Lite, was used for this research. The SUV model that was used to create the interview questions were also used to categorize the collected data. This model takes a systems-based approach and is derived from GST (Jokela et al., 2008) thus linking it to the conceptual framework. It consists of three levels and seven categories. The three levels are individual, technology, and organization. The seven categories are goal seeking, regulation, hierarchy and relations, differentiation and entropy, transformation process, input, and outputs (Jokela et al., 2008).

The first step was to categorize and compose the data. This step included the interviews that were conducted, and audio recorded for transcription using oTranscribe. The research logs were completed during the interviews as well as at the time of the transcription to further compose the data. At this point, member checking was completed allowing review of validated

information in the next step. This step also included generation and categorization of the information into the different levels and categories identified by the SUV model. Actual placement of the data into levels and categories did not occur until step three. The data was organized for easier review using QDA Miner Lite.

The second step was to read over all the data. In this step, the transcriptions were reviewed, along with the research logs and the notes composed in the previous step. This step was simple as it was merely reading and comprehending all the data that had been collected from all the research participants. This step was followed by the initiation of the coding process.

The third step, being the coding analysis process, is where Tesch's eight step coding process came into play. First the information was reviewed to get a sense of the entire subset of data. This was just a repeat of step two listed above. The next requirement was to choose a document and get an understanding of its underlying meaning. One of the research participant's transcripts, along with any relevant information about that interview from the research log and written notes from prior steps, was examined to gather a more thorough understanding of what the interviews had uncovered. Developing major topics by repeating the previous step for several research participants was the next step. After the review of the selected research participant data was complete, the next step was to create an initial coding scheme. Since the SUV model already had provided the study with levels and categories, the coding scheme coincided with that setup. Codes were created for the individual, technology, and organization levels along with the seven categories of goal seeking, regulation, hierarchy and relations, differentiation and entropy, transformation process, input, and outputs. Information that was uncovered but did not fit into the seven categories was still classified under one of the three levels, but into an appropriate category I created. Once the codes were created, the data was grouped into the appropriate categories.

Completion of this step allowed me to finalize the category abbreviations and organize them accordingly, which was the next step. After gathering all associated data with a code in one location to begin analysis, anything that needed recoding was recoded. This completed all eight steps recommended by Tesch.

The fourth step in this data analysis process was to generate descriptions, categories, and themes during the coding process. This had mostly been predetermined by the SUV model. Any additional categories were added at the end of step three based on the steps provided by Tesch. Step three and step four coincided perfectly. During this step, all the categories and levels were double checked for accuracy and appropriateness. The fifth step was to propose the descriptions, categories and themes that were embodied in the qualitative account. This step allowed the categories, both pre-determined and emerged, to be connected. Any categories that developed from the data analysis were examined thoroughly making sure that all the data was properly categorized. This step acted as a check and balance for step four.

The final step was to make an interpretation/explain the meaning of the data. This last step was where the data was explained. Here was where reports and tables were fashioned to explain the data in plain terms. All conclusions drawn and all findings were noted and demonstrated in this step. After the reports and tables are created, they were double checked and assembled for reference. Finally, overall, data analysis (presentation, interpretation, explanation) was consistent with the research question and underlying conceptual framework of the study.

Reliability and Validity

Trustworthiness can be established in research when dependability, creditability, transferability, and confirmability are measured (Capina & Bryan, 2017). Dependability in qualitative research refers to the ability to be able to track the procedures that are used in a study

to gather and interpret the data (Browne, 2018). With this study being qualitative, member checking was used create trustworthiness in the research and mitigate any researcher bias that could surface (Candela, 2019). Member checking took place during the transcript review process to verify that the information captured from the research participants was accurate and reflective of the participants' actual stance on the topic being studied. Validity can be achieved in research when and if a pilot study of research instruments is conducted (Dikko, 2016), therefore this study implemented a pilot study to enhance research dependability.

Some of the utmost threats to creditability in qualitative research are the researcher's inability to avoid bias, remain creative in their inquiry, and to stick to the rigorous steps of the chosen research method (McCormack & Thomson, 2017). Member checking helps to avoid bias in qualitative research. It is cited as being the most significant means of ensuring creditability for a qualitative study (Woith, Kerber, Astroth, & Jenkins, 2017), therefore member checking of transcribed data was done for this study to ensure creditability. Triangulation is listed as the most customary credibility technique to employ (Liao & Hitchcock, 2018), making the use of the multiple data source triangulation data analysis process for this case study a means of ensuring creditability as well.

Transferability broaches the possibility that the results and conclusions of the study will remain valid in other situations (Cafarella, 2016). Transferability is a conclusion drawn by the reader to regard a study as reasonable or not and is therefore not defined by the researcher (Krupic, Eisler, Sköldenberg, & Fatahi, 2016). Lincoln and Guba, 1985, stated that one strategy that can be used to address transferability is thick description. Thick description was used to address transferability in relation to the reader and future research. Detailed information about the attitude of the participant and other factors were important to developing a thick description for

the readers (Amankwaa, 2016). Keeping the research log as detailed as possible assisted in that endeavor.

Confirmability is defined as the level of which findings in a study are developed by participants as opposed to researcher bias or personal motivation (Amankwaa, 2016). Triangulation is often used to establish confirmability in qualitative research (Pryce et al., 2019), therefore the use of triangulation in the study assisted in addressing confirmability. Keeping the research log as well as conducting member checks also contributed to addressing confirmability in this study (Connelly, 2016).

When conducting qualitative research, the issue of reaching data saturation surfaces when interviewing participants (Fusch & Ness, 2015). Saturation is used as a measure for discontinuing data collection and analysis (Saunders et al., 2018). Data saturation is reached when there is sufficient data to reproduce a study, the capability to acquire additional information has been achieved, and when additional coding is no longer practical (Fusch & Ness, 2015). Data saturation was ensured in this study by exhausting all viable participants in the target area and verifying that all data points are thoroughly documented for future replication.

Transition and Summary

This section of the study evaluated the role that the researcher plays in the study along with the means of managing the participants. The research method and design chosen for this qualitative study further expanded on the information provided in Section 1. Next, the population and sampling methods were explored, followed by a listing of ethical considerations to be taken during this study. The data collection, organization and analysis techniques selected for this study were mentioned and the section concluded with an explanation of how this study will achieve reliability and validity.

Section 3 contains the results of the study based on the data collected from the research participants. It will also discuss the applicability of the findings with respect to the professional practice of IT. This information will be followed by implications for social change and recommendations for action and further research. My reflections will be followed by a conclusion of the document.

Section 3: Application to Professional Practice and Implications for Change

The focus of this study was exploring the security strategies that university data custodians use to protect data. This section contains information referencing my findings at completion of the study and how the findings can be effectively applied to the professional practice of IT. Five major themes emerged from the data, showing the importance of adaptive security measures, buy-in and/or resources, proper management and personnel, state/industry regulations adherence, and SETA. The findings both confirmed and extended knowledge in the IT field. Comparing the findings with peer-reviewed studies from the literature review and other existing literature illustrates how the findings advance the field of IT. In this section, I also address the positive implications for social change along with a recommendation for action. This section will conclude with recommendations for further research, reflections on the research, and formal study conclusion.

Overview of Study

The purpose of this qualitative case study was to examine the information security strategies that university data custodians use to protect PII collected from staff, students, and other stakeholders. The data from this research came from conducting semistructured and online conferencing interviews. The findings allowed major themes to emerge showing the importance of adaptive security measures, buy-in and/or resources, proper management and personnel, state/industry regulations adherence, and SETA. This section begins with a brief overview of the method in which this study of security strategies was conducted. It will be followed by a review of all questions, exploration of any issues, and a summary of all findings.

Presentation of the Findings

The overarching researching question was: What information security strategies do university data custodians use to protect PII collected from staff, students, and other stakeholders? To answer this question, I conducted 15 semistructured interviews with data custodians. The targeted population consisted of data custodians from various universities and colleges in North Carolina and South Carolina who have an implemented set of security strategies. The results were analyzed using QDA Miner Lite where coding of the interview transcripts took place. That coding resulted in the emergence of five key themes: (a) adaptive security measures, (b) necessity for buy-in and/or resources, (c) proper management and personnel, (d) requirements based on state/industry regulations, and (e) SETA. These five themes exemplify potential strategies that could be used for implementing security strategies at other higher education institutions.

Theme 1: Adaptive Security Measures

The first emergent theme from the collected data was the implementation of adaptive security measures as a security strategy. Providing adaptive security measures is important because the threat is everchanging and the security measures in place to protect PII should be malleable and vast enough to thwart various types of attack. According to the study findings, the interview participants implemented various adaptive security measures to protect university PII. These security measures varied in intrusiveness, frequency, and reasoning.

In 11 of the 15 cases, data custodians indicated that data breaches at other universities taught their institution a lesson. Although this measure is not actionable for implementing change, it does heighten awareness and could potentially result in changes based on the evaluation of the lesson learned. Participant 10 indicated that their institution pays attention to incidents that occur

at other universities, particularly institutions that use similar software. Looking into this software would have the potential to allow the data custodians to identify issues that may not have been checked for prior. It would also allow the data custodian to verify that the measures in place are acceptable, thus providing a necessary assessment of existing defenses. Participants 5, 9, and 11 all indicated that learning from data breaches that occurred at other universities did not result in an amendment to their existing strategies, but more so an internal assessment to verify they were doing what was necessary to keep from suffering the same fate. The other participants echoed the sentiments, adding that breaches at other universities helped their institution be more proactive and preventive and to increase communications within the ranks to make sure that all personnel are on the same page.

Other participants indicated that they either focused on various attack types/vulnerabilities or made general improvements or limited access for users because of other university data breaches. Phishing and ransomware were both attack types addressed by many of the interview participants. One third of the participants indicated that phishing and ransomware attacks were the reason their information security strategies were examined, thus providing verification that the adaptive security measures in place to impede institutional data breaches were indeed effective. Another third of the participants indicated that continuous improvement, awareness, and limiting access were their reactions to data breaches at other institutions. These adaptive measures are important because any security measure set up to aid in protecting PII needs to fluctuate as outside threats change.

When I asked the participants to specify which security strategies were the most beneficial in providing data security for their university, a third of the participants stated that the most beneficial security strategy was multifactor authentication (MFA). Participant 13 stated that

MFA was mandatory at their university. Duo, one of the multifactor companies identified by Participant 13, is Cisco's user-friendly, scalable access security platform that keeps businesses ahead of ever-changing security threats. Duo provides reports to the data custodian when an anomaly is discovered. Participant 6 indicated that MFA was in the process of becoming a requirement for all students; MFA essentially reduces the number of compromised accounts. Participant 9 indicated that MFA is key regardless of the type of organization because if MFA is not a part of the equation, it is ultimately not safe. Participant 9 agreed with Participant 6 that MFA is important because it is demonstrated to significantly reduce the risk of compromised accounts.

The remainder of the data custodians had a variety of adaptive security measures in place to protect their universities' PII, including simple and brief security policies, properly executing the basics, increasing password complexity, focus on preventing attacks, enhancing account security, having an effective response method in place, 0 trust, port security and proper authorization, and monitoring. None of these responses stood out individually, but all of them make an impact on the security of PII at the respective institutions of these data custodians according to their responses. Participants 8 and 15 agreed that brevity in security policies was important because for users to follow a policy, it must be simple, easy to understand, and even easier to execute. Participant 12 stated that password complexity for their institution included using different passwords for different systems. Participant 8 revealed there are a lot of fancy technologies out there for security that can be used, but if their institutions were to use all of them without properly executing the basics, there would still be the potential for exposure. In regards to focusing on preventing attacks, Participant 13 acknowledged that account takeover has been a primary focus because their institution has so many individuals with accounts, thus providing a large attack surface that would allow an intruder to gain a foothold in the institution. With the

variety of responses for this question, it was clear there is no one way to protect PII at universities. The multitude of strategies reveals that it is important to do what works for each institution and to make sure that whatever security measures implemented are nothing short of adaptive.

Regardless to how adaptive a security measure is, it must be evaluated and updated at some point to remain useful and relevant. When the data custodians were asked about the frequency in which their security strategies were updated, many responded saying that the strategies themselves were not changed. What was changed were the means of execution. Once the participants began to elaborate, nine out of 15 participants indicated that their strategies, or at least their means of executing their strategies, were updated annually. When looking at the other responses, there was a bit of overlap. The initial response may have been as needed, but out of the six participants who responded that their security strategies were updated as needed, all but one participant gave a concrete numerical response indicating either biannual, annual, or twice per year for strategy updates. There were three participants who indicated their policies were not updated enough. Participant 1 felt that attrition attributed to the lack of timely updates. The institution's policy calls for updates at least every 2 years, but with changes in leadership, disjointed documentation, and massive policies that are out of support, the 3- to 4-year range was more on the mark. On the other side of the spectrum, there were several participants who indicated they do periodic examinations of the strategies while only making modifications if necessary.

The final element of this theme of adaptive security measures surfaced when the data custodians were asked about the method and frequency that is used to measure the effectiveness of the security strategies implemented in their institution. Vulnerability management was the top

response to this interview question being the measurement for four of the 15 participants. The success of Participant 1's strategies were measured by the turnaround times of their vulnerability management. The faster vulnerabilities were remediated, the more successful the program is being. Reporting, other data incidents, and penetration testing were the third most popular replies. 20% of the participants indicated one of these methods of measurement as their primary method to determine success of their implemented strategies. Reporting from Microsoft exchange and Akamai allowed Participant 7 to judge the effectiveness by examining how many bad locations were being accessed and how many bad protocols were being attempted. Akamai, the leading content delivery network services provider for security solutions, provides web and Internet security services. Participant 15 indicated that the number of data incidents that occur are a primary measurement for their institution which was echoed by Participant 2 and Participant 8. Penetration testing, not to be confused with vulnerability assessment, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system. This method was used by Participants 7, 12 and 14. Participant 14 even does surprise pen testing annually for their IT department.

The other responses to this question that related to adaptive security measures were to measure using maturity ratings, risk management and incident management. In looking at the responses to this question, just as the responses to the question of the most beneficial security strategy, it is evident that there is not one particular way that is best to measure the effectiveness of a security strategy as long as there is a measurement in place that works for the composition of the institution. Another finding when looking at the responses was that many of the data custodians did not have just one method in place to measure the effectiveness of their strategies. Of the 15 participants, 87% of them responded with multiple methods of measurement. Participant 10 listed auditing, surveys, downtime tracking and incident reports as implemented

measurement methods. The frequency in which these methods are measured was almost unanimously throughout/continuous with 93% of the participants providing this response. Participant 5 stated that their institution begins with a plan. They look to see what they are going to do, gauge against their progress, and then they do have regular intervals where they go back and look at those retrospectives.

The above findings both confirm and extend knowledge in relation to InfoSec within IT. According to information researched during the completion of the literature review, to properly develop an ISP, there are several factors to focus on to make the policy comprehensive including password management, email/internet use, social media use, mobile computing, and information handling (Alqahtani, 2017). Each of these elements were addressed, outside of the social media use directly. Participants allowed this study to extend knowledge by indicating other factors that need to be implemented for policies to be considered as comprehensive. Oklahoma State University concluded that the number one reason for breaches in data via account access was the strength of the password (Farcasin & Chan-tin, 2015) as mentioned in the literature review. This research showed that university data custodians are aware of this issue as password complexity was identified as one of the adaptive security measures implemented to protect university PII. The literature review also indicated Doherty et al. (2009) conducted research that revealed of their 122-university data sample, only 61 had current ISPs that were readily accessible online. During this research, data custodians from over 200 universities and colleges in North Carolina and South Carolina were solicited to participate. More than half of those universities had current ISPs readily accessible online; however, one thing that was noticed is that many of them did not directly identify the individuals responsible for not only the policies, but also for the protection of PII at the institution. There was a lot of research and networking required to gather this

information. In compiling the list of institutions to solicitate participation, to date, I was unable to identify their appointed data custodians.

GST was used in this study as the conceptual framework to delve into the correlation between data custodians, security strategies and the implementation of security strategies at various colleges and universities. The findings that fall under the theme of adaptive security measures relate directly to the hierarchy principle of GST. The hierarchy principle proposes that objects treated as a whole are made up of smaller objects, which are to be regarded as wholes in themselves (Whitney et al., 2015). Each of these adaptive security measures are smaller objects that are treated as their own understanding that they make up a whole defensive system for colleges and universities. MFA does not stand alone. When MFA is implemented, it stands alongside password complexity as a requirement, frequently updated security strategies, reporting as a method of measurement that is continuously measured to judge its effectiveness, all due to a need to protect university and college PII. Without anyone of those elements, protection of that data could fail.

Adaptive security measures are effective in modifying a system's security based on the nature and intensity of threats that are being met (Ahmad, Malik, Alreshidi, Khan, & Sajjad, 2019). New peer-reviewed literature is still very scarce. This research will assist in filling the gap in literature that addresses InfoSec at colleges and universities. With that information, there are new pieces of literature that have been published that do address InfoSec within large organizations. The new pieces of literature do not dispute any of the findings in this study. Chung (2020) stated that cyber security is not something that you can set up and not revisit. With only 3% of the world's organizations prepared to defend against certain attacks and with cyber criminals becoming more advance, Chung (2020) indicates that organizations must use a strong

set of adaptive security measures in their strategies. Tariq, Asim, and Khan (2019) echo these same sentiments in their research stating that strong, adaptive security measures are required to defend against innovative attacks.

Theme 2: Necessity for Buy-in and/or Resources

The second emergent theme from the collected data was the necessity for buy-in from leadership, staff, and students as well as the necessity for resources, both financially and personnel wise. Obtaining buy-in from leadership is important because leadership solicits the financial resources to execute a requirement. Without those resources, requirements go unfulfilled thus leaves data vulnerable. Buy-in from staff is required because the staff acts as the executors of the requirements. If they are not on the same page with the data custodians, their lack of knowledge, understanding, or even willingness to properly execute a task would render data vulnerable. Buy-in from students is required because students are at the forefront of data transmission. If they do not acknowledge a need to secure their data, there is no way for data custodians to effectively do their job, which is to protect data throughout the institution. Having the financial and personnel resources to execute a requirement is crucial. Data protection efforts cost money, personnel must be paid their salary, and that same personnel must be on the ground executing the requirements necessary to protect institutional data.

Seven of the 15, or 46.7%, of the data custodians revealed that new threats were one of the leading external factors that played a role in deciding what strategies to implement within the university. The main reason that buy-in is a necessity is because many of the data custodians mentioned that they were in a consortium with other universities in the area. Without having buy-in from leadership, when a college or university states that there is a new threat that could potentially affect the consortium, hundreds of thousands of records then become vulnerable. To

put this into perspective, consider I interviewed 15 data custodians from different sized colleges and universities. The average size of these 15 institutions is 15,772 students. This means that if each of the institutions were this size, the data of 236,580 students would be at risk. If each student requires both parents' information on all documentation, the original number triples to almost three-quarter of a million people at risk. These numbers are only referring to 15 institutions. The consortium consists of over 100 institutions and some of these institutions are significantly larger than the average number listed. This number only accounts for currently enrolled students. It does not account for alumni, staff, faculty, and donors which would substantially increase that number.

The other answers of new technologies, institutional budgets/resources and culture were almost equally divided amongst the participants. Participant 1 stated that technology and how it develops along with the availability of new technologies and the development of new technologies tend to be external. Since institutions do not develop a lot of their own technologies, they are more inclined to use technologies that are available everywhere. Participant 9 added to this thought pattern by adding that if you look at where institutions are today and compare it with where an institution was a few years ago, sometimes they are not even running the same caliber of technologies or systems available in the past. This means that the security posture should be completely different than it was in the past. Institutional budgets/resources were a very hot topic that came up with every participant during this study. Participants 1 and Participant 8 agreed that many data custodians do not have the proper financial nor personnel resources to handle every possible problem that exists. State funded institutions rely on appropriations and budgets that will allow them to do what they need to do to protect university data. When the state makes changes, especially when there are budget cuts, they directly impact on what the institutions work on, how many people they must work on that task, and the types of technologies they are able to purchase

and implement. Participant 5 was one of the participants that referenced culture as an external factor by replying that they have many different cultures at their institution, so one change may mean one thing to one group and a different thing to another. It is important to have buy-in from leadership, especially actors at the state level that make university budgets, because without the proper funds to invest in new technologies and pay salaries, all the points made by the participants above are forgotten.

The participants were given a follow-up question asking if the external factors cause challenges or make it easier to implement security strategies. While 40% of the participants indicated that their external factors cause challenges with implementation, 27% indicated that their external factors make implementation easier. Five of the participants, or 33%, indicated that their external factors both cause challenges while at the same time they make implementation easier. There was not a true outlier in the response to this question. Many of the participants indicated that state mandates and the state budget were what caused a challenge. Participants on the other side of the response pointed out that the external factor of state guidelines made their job much easier. The 33% of participants that stated external factors both cause challenges while at the same time they make implementation easier mentioned both the state budget and the presence of a set of guidelines as their reason for splitting their answer.

When the participants were asked what prompted them to implement their security strategies, half of the responses fell into this theme. A third of the data custodians identified security threats and breaches as the reason that their institution implemented its security strategies. Participants 1, 7, and 8 agreed that the evolution of technology has made it so that an institution cannot have technology and not pay attention to security. Observations of things that have happened at other places, along with observations at their own institution made it clear what

the needs of the institution were in terms of maintaining the security of technology and information resources. This leads into the next response which was that previous incidents were the reason that the data custodians implemented their current security strategies. This response, along with internal reflection and new policies and procedures, showed that there are a variety of reasons to get buy-in and resources. It is also imperative to have enough personnel to be able to manage new policies and procedures that come down the pipeline as a mandate. If leadership is not able to recognize the need for a piece of software meant to aid in preventing a recurring incident, whether that occurred at the university or at a neighboring institution, the incident has the chance to occur again. It is also important to point out that leadership not buying in to what the data custodians are presenting as a potential issue prior to occurring forces the data custodian to be reactive instead of being proactive. This was something brought up by a couple of participants as a concern.

There were three questions that continuously rendered the same response from the participants. When asked how data breaches at other universities caused their institution to amend existing security strategies, if they were involved in the process for choosing who modifies the security strategies, and if there was any additional information to provide surrounding security strategy implementation, the data custodians echoed each other in their responses by referring to different levels of buy-in from different individuals. Participant 4 stated that incidents at other institutions drew the attention of leadership as well as justified an institutional need by making it evident to the university president that security governance was a necessity. Participant 3 reiterated the sentiment of Participant 4 by stating that incidents at other institutions drew the attention of leadership as well as justified an institutional need which resulted in an additional allotment to the university additional funding to implement better security appliances. The need for buy-in is important because, unfortunately, until an incident of some sort occurs, the threat is

invisible. As stated before, buy-in from leadership from the start will allow a university to be proactive in their defense against various threats. Participant 15 got buy-in from their college so that they were able to come in and state exactly how the security operations were going to go. This aids data custodians with the execution of their job duties because now their actions are validated by the leadership at the institution. Eleven participants afforded me a response when asked to provide additional information surrounding security strategy implementation. Every one of those responses referred to the necessity for buy-in or for resources as these topics were not blatantly addressed in the interview questions. Participants 4, 6 and 14 indicated that funding is the primary thing that gets in the way of providing proper security for their respective institutions. Participants 6, 8, and 10 stated that user buy-in is extremely important. This will be explained in further under the SETA theme but was necessary to mention here and buy-in is not only a necessity with leadership, but also with users. Participants 7 and 11 agree that having enough personnel resources is an important element in security posture. Participants 1 and 5 pointed out that colleges and universities have a culture that is resistant to change, while Participant 6 pointed out that those same colleges and universities need to give buy-in to their individual IT departments to know they are supported.

The above findings continue to confirm knowledge in relation to InfoSec. They remain consistent with information researched during the completion of the literature review. On the InfoSec management side, to properly implement an information security strategy, corporations must have the support of leadership responsible for development of said strategies (Montesdioca & Maçada, 2015). On the InfoSec compliance side, research shows that to properly implement an information security strategy, corporations must have the support of leadership responsible for the development of the strategies (Montesdioca & Maçada, 2015). Studies, including this one, show that there is a significant relationship between support of leadership and ISP compliance

(Flowerday & Tuyikeze, 2016). As stated before, buy-in not only reassures the IT department that they are supported, it also presents a united front to other users. Without buy-in from leadership, many threats can go undefended creating a massive issue for IT professionals if an incident were to occur. In Table 1, administrative cost was listed as a recurring cost. What Table 1 does not show, and what this research suggests, is that the number of key personnel required to do a job adequately needs to be considered. The final calculation of salary multiplied by the number of resources should match the budget for administration so that the proper number of resources can be allocated to each institution.

The findings that fall under the necessity for buy-in and resources theme relate directly to the holism principle of GST. The holism principle states that a system should be regarded as a whole, not as summation of the individual parts (Whitney et al., 2015). The contextual axiom that supports this principle states that the meaning of a system is defined by factors surrounding the system (Whitney et al., 2015). Buy-in on all fronts along with resources on hand are concepts surrounding the very feat of security strategy implementation. Applying this GST principle adds more criticality to the concept of this necessity because this means that the implementation of a security strategy into a system is not complete unless there is buy-in and available resources.

New literature points out that a project will more than likely be fruitless if individuals that represent the business do not participate in a given project since business management buy-in is vital for any security funding and policy implementation (Spears, 2018). Panahifar and Shokouhyar (2019) found in their research that senior management support is one of the foremost enablers which lead to all other study enablers resulting in competitive advantage. From further analysis of this phenomenon, it was argued that leadership plays a critical role in successfully managing teams and appropriately encouraging an internally and externally collaborative

atmosphere (Panahifar & Shokouhyar, 2019). Studies conducted in 2018 revealed that an organization will be vulnerable to cyber-attacks if there is a lack of personnel that are knowledgeable in applying InfoSec safeguards (Kam, Menard, Ormond, & Crossler, 2020). Astakhova's (2020) research reveals that one of the issues in the culture of InfoSec is the lack of personnel who can solve InfoSec concerns, which is true both at the organization level and at the mass level. This research supports the findings and validates the necessity for buy-in and for resources.

Theme 3: Proper Management and Personnel

The third emergent theme from the collected data was an emphasis on proper management making decisions with proper personnel carrying out given requests. The importance of buy-in and personnel as a resource has already been addressed in this study. This theme addresses the result of achieving the necessary support from leadership. Once an institution has the personnel required to complete any given tasks, there must be a system to place that places personnel in the right position to be effective. This is the case for both management and subordinate employees. Several of the interview questions resulted in replies that specified the importance of proper protocol when regarding the involvement, selection, and placement of various personnel.

I posed questions inquiring about the most beneficial security strategies as well as what prompted the implementation of the current strategies in place at the college or university. Some of the responses fell into other themes. Sixty percent of the participants' responses to these two questions pointed out that the most beneficial security strategies were properly managing rights and proper access along with ensuring proper personnel are the individuals making the decisions, while the creation of the data custodian's position along with a governing decision made by

leadership prompted the implementation of the current security strategies. The principle of least privilege is the method that is used by Participant 8's institution. According to Participant 8, principle of least privilege within the institution allows access to data solely based on an individual's role and responsibilities. Following this principle keeps data out of the hands of just anyone. Limiting data handling ultimately limits the possibility of unwanted data exposure. The culture at Participant 9's institution allows the technical experts to verbalize their innovative ideas. This organic means of innovating materializes when an institution's culture is nimble, able to accept good ideas, and allows those ideas to be put in place. The leadership at Participant 5's institution recognized the importance of security and that they were falling behind other institutions that had already implemented security programs. An understanding about how critical the data was to the business of the institution led to the hiring and placement of Participant 5 into a leadership position that had not existed prior to their arrival. Participant 11 echoed the same sentiment avowing that their leadership position did not exist prior to their arrival either. There had been a lot of decentralized IT functions, but no centralized coordination, so when Participant 11 arrived and learned that there was not a formal security program, that is when the security strategies began development and implementation.

Eighty percent of the participants were completely involved in the process for choosing which individuals modify the institution's security strategies. Participant 8 had a few integral members of their IT staff chosen prior to their arrival, but since their arrival, they have been completely involved in the hiring process. This is important because the data custodians that participated in this study have a complete understanding of the inner-workings of the institution's data security program, which means that when an institution is hiring for a position, the data custodians would be able to pinpoint how and where the hired individuals would fit. Participant 12 had not been at their institution for long, which is why their team was chosen before their

arrival, but when working at other institutions, they were completely involved in the hiring process. Participant 11 had been at their institution for a while, but still had members of their team that were chosen before their arrival as well.

When many of the participants were asked specifically about the process used to select those individuals, they identified several different methods. Forty-seven percent of the participants used inherit job responsibilities as selection criteria when selecting from internal candidates. There was no mention of a formal identification or selection process. Participant 7 uses availability as a determining factor, which puts more emphasis on the importance of having enough personnel. Participant 1 leverages their internal team and chooses based on job responsibility. When using an external selection process, other participants use a committee to choose the individuals that come onto the team. Participant 4, who uses job responsibility to select internal candidates, uses a committee when selecting external candidates. Participant 12 uses multiple committees depending on the job duties. Participants 14 and 15 responses were the outliers for this question. Participant 14 chooses based on skill set instead of job responsibility. Participant 15 created their process from scratch as there was no formal process prior to them coming to the institution. One thing that stood out with this question is that 80% of the participants indicated they were in some way involved with the process for choosing personnel also indicated they have a committee to help choose new team members. This statistic stood out because, although the participants may see the full picture regarding the institution's data security program, there may be some nuances between what occurs and what is perceived to occur in each position; therefore, it is a good idea to have the entire team involved in the choosing of new personnel. Structure is required during the hiring process, while assigning personnel to a job, as well as with the individuals required to manage all these processes.

A centralized management structure is defined as the presence of an essential stakeholder that is involved in major decision making (Fontainha, Leiras, de Mello Bandeira, & Scavarda, 2017). A decentralized management structure, on the contrary, has no single organization or agency with authority over other organizations (Fontainha et al., 2017). When asked if the participant's university has a centralized or decentralized management structure for data custodians across campus, the responses were almost split. Half of the participants stated that they have both a centralized and decentralized management structure within their institution. Participant 6's institution had a decentralized structure for their data custodians and a centralized structure for their data stewards. Participant 9 used both management structures citing that differing areas of their data governance system have differing managing structures. Sectors such as HIPAA, FERPA, and PCI all have different individuals managing the compliance efforts, but none of the areas go unmanaged. The remaining participants selected one management structure or the other. Participant 5 used a centralized structure where everyone is under the same data governance standard with the same role and the same expectations. Participant 2 had a decentralized management structure with some coordinating committees trying to standardize it. With this question, there was not a right or wrong answer. The question was posed to get a better understanding of the crux of the institution's implemented data security program.

These findings extend knowledge in relation to InfoSec. While reviewing the literature, InfoSec management was discovered to consist of several components including properly informing the managers and users of new operations. For individuals to be properly informed, the data custodians relaying the message must have a clear understanding of the information. Structure being rendered at the hiring, assignment and management phases within an IT department allows adequate passage of information. Companies have trouble identifying which department is responsible for implementing a developed ISP (Fazlida & Said, 2015). This

identifies the importance of having an established management structure. Given the results of this study, there is no necessity to choose a particular structure, but there is a necessity to identify and select one that works for the data custodian's individual institution. Some corporations allow responsibility to rest completely on technical managers and upper management, namely Directors, pay little attention to the process (Fazlida & Said, 2015). There is also the issue with relying primarily on technical solutions which makes a corporation rely too heavily on technical controls, meaning more responsibility for the technical staff (Fazlida & Said, 2015; Sohou & Holtkamp, 2018). If there is going to be more responsibility on the technical staff, then there needs to be staff in place that can handle the work assigned to them. InfoSec customarily has been reliant on insiders, or employees, making proper security decisions (Thompson, 2013). The employee, whether management or subordinate, needs to understand what their position entails to be able to make these decisions. This highlights the importance of hiring proper personnel and having the appropriate individuals making InfoSec program decisions.

The findings within this theme directly relate to the centrality axiom which is supported by the hierarchy principle and states that the levels in a system's hierarchy are based on the development of sublevels (Whitney et al., 2015). The sublevels being addressed in this theme are the different stages of the hiring process, the differing ways that each institution completes their hiring process, as well as the process of assigning hired individuals to a position that fits their skill set. Systems-based approaches when referring to complex situations involving decision making enables the decision makers to address the situation fully (Yurtseven & Buchanan, 2016). The goal of GST is to methodically determine a system's inner workings such as subtleties, restrictions, conditions, and ideologies that can be distinguished and applied to systems on various levels. These points about GST show how the elements of this theme meld with the chosen conceptual framework.

As Rizvi, Pipetti, McIntyre, and Todd (2020) posed in their research, the possibility of a breach is possible; therefore, proper personnel must be carefully vetted and organized for securing different kinds of data. New peer-reviewed literature shows that the selection process can be overwhelming but is essential in recruiting proper personnel for specific jobs (Lugo et al., 2019). Proper personnel management will guarantee suitable recruitment, selection, placement, and orientation of employees into their specific duties (Okanazu, Madu, Igboke, 2019). For example, selecting the correct employee and assigning them to the correct positions at the precise time needed, will result in the success of the organization (Okanazu et al., 2019). This research supports the findings and validates the necessity for proper personnel and management.

Theme 4: Requirements Based on State/Industry Regulations

The fourth emergent theme from the collected data was the prominence of adhering to industry regulations that were passed down by the state as a mandate. The need to adhere to state and industry-based requirements provided an additional duty for data custodians to consider when protecting university data. According to the study findings, many of the participants were mandated by the state to some capacity to incorporate different frameworks such as the NIST 800 series and the International Organization for Standardization (ISO) 27002 standard. Surveys, annual audits, annual assessments, and gap analysis were used by the state to measure the effectiveness of security strategies at these various universities. One element of this theme that supplements the understanding of the data governance operations of an institution is how the state uses institutional occurrences within a consortium to regulate requirements that are passed down as mandate.

Many of the responses to the interview question asking participants how data breaches at other universities caused amendments its existing security strategies at their institution fell into

the adaptive security measures theme. There were a few responses that fell into this theme, namely the responses from participants 1, 4, 5, and 8 that identified institutional collaboration as a reason for making amendments to their security strategies. Participant 1's institution frequently collaborates with the information sharing accountability centers of other institutions. It should be noted that when an incident is brought to the attention of the data custodian at the university, a broad view is maintained so that all controls continue to get attention when leveraging the information relayed by other institutions in reference to incidents that have occurred. Participant 5 noted that working in the consortium with other universities serves as a great benefit when it comes to information sharing. When any of their institutions have an issue, others are very willing to share what happened along with the root cause analyses. Getting first-hand information from other trusted data custodians is a great way to do a check and balance on existing strategies to make sure that the same vulnerabilities do not exist with the purpose of avoiding the same fate.

An audits and mandates are both great reasons to implement security strategies. Seventy-three percent of the participants identified one of these two options as reasons for putting certain strategies in place. Participant 9 raved about the internal audit team at their institution, dubbing it a very transformative department that really makes things happen. The internal audit team was labeled fair, engaging, and supportive while insuring accountability and appropriate controls. Participant 9 recommends auditing to ensure objectivity, something that many IT teams really need. Participant 12 agreed adding that their institution has both security and financial audits to help gain perspective when putting strategies in place. As stated before, many of the data custodians' institutions are in a consortium and their mandates are passed down by the state for each institution to implement accordingly. The colleges and university data custodians have an obligation to the state and a requirement by the state to secure infrastructures and data. As stewards of data, they have a responsibility to guarantee the integrity and security of that

information. Participant 4 articulated these facts to show how the mandates influenced implementation at their institution. Participant 14 reverberated that sentiment simply stating that the law mandates these requirements, and since the institutions are governed to have them, that is what is done.

State mandates, other institutions, external firms, and existing frameworks and standards were all identified by the participants as external factors that play a role in deciding what strategies to implement within their college or university. Sixty percent of the participants said that state mandates were an influencing external factor. Participant 3 had periodic audits of security by the state that influenced continuous evolution. Other participants had differing state mandates, but all revolved around a check and balance that forced their IT departments to stay on top of their implemented security strategies. Information sharing between other universities, as well as external firms, was a guiding external factor for both Participant 13 and 14. As mentioned before, the ability to share information between institutions allows a more collaborative effort to thwart attacks. Participants 6, 7, and 15 all agree that along with state mandates, outside frameworks and standards were guiding external factors for security strategy implementation.

This brings us to the next subset of elements within this theme which resulted from the questions posed asking which security strategies were the most beneficial and if the data custodian's university developed security strategies based on a particular framework or standard. Two of the participants identified using a particular framework as the most beneficial security strategy at their institution. Comprehensiveness is important and Participant 1 stated that if one does not have a framework to work off, then that comprehensiveness may be lacking as that is what the framework is to provide. Participant 1 went on to state that leveraging the ISO 27002 control set has been very beneficial because it helped make sure that everything that needed

attention got attention. Participant 12 used the NIST framework instead of the ISO control set. The specific NIST framework was not identified. The NIST 800 series, used by 73% of the participants, and ISO 27002, used by 46.7% of the participants, were only a couple of the frameworks and standards used by data custodians. It should be noted that six (6) of the participants used both NIST and ISO, which would explain the disproportionate percentages reported. PCI, the Gramm-Leach-Bliley Act (GLBA) standards, gap analysis, and the Center for Internet Security (CIS) top 20 were all identified by 20% of the participants as standards and frameworks consulted at the institution. GLBA is also known as the Financial Modernization Act of 1999 (Binkley, 2016). GLBA is a U.S. federal law that mandates financial institutions to clarify how they share and safeguard their customers' cloistered information (Binkley, 2016). These results show what the state has included in their mandates, but also give a peek into some of the obstacles that data custodians must surpass to meet the given mandates. These frameworks are public knowledge and available for view in depth at any time.

The final element of this theme was formulated with responses to the interview question asking what method of measurement is used to determine the effectiveness of security strategies. Surveys and audits were not only prompts for implementing security strategies; they were also a means of measuring effectiveness for 33.3% of the participants. Audits were the main means of measurement for Participant 4. A clean annual audit was used as both a safeguard and proof that the institution adhered to all state mandates just in case an incident did occur. Participant 10’s institution used regular IT security audits along with organization wide satisfaction surveys. These surveys verify that systems are available and perceived of as being secure and usable, which in turn measures effectiveness. External standards, annual assessments, and gap analysis were used by another 33.3% of the participants. Participant 1 used both external standards and gap analysis for measurement. The ISO framework was one of the external standards mentioned

in the retort. Another standard that was used was the CIS Critical Security Controls (Woods, Agrafiotis, Nurse, & Creese, 2017). The CIS' Critical Security Controls Top 20 Controls provide a more detailed perspective in comparison to the ISO framework and can be essential at identifying infrastructure vulnerability (Woods et al., 2017). Gap analysis was used by Participants 1 and 9 to measure controls across the board. Participant 13 used the annual reviews to measure effectiveness. The goal for the institution is to complete both an internal and an external assessment on opposing years. These responses further knowledge on means of measurement by indicating, as with the other information provided, that there is no one way to measure effectiveness as long as there is a measurement in place.

The findings in this theme confirm knowledge in relation to InfoSec compliance. In the literature review, it was noted that proper InfoSec conduct lessens the risk of a data breach in organizations (Safa et al., 2016). InfoSec compliance allows organizations to audit practices and determine if the organization is adhering to defined controls (Choi, Martins, & Bernik, 2018). The results of this study show various ways to audit practices and determine if the institution is adhering to the defined controls passed down by the state. Compliance with ISPs can have a direct effect on the success or failure of an Information security strategy and policy; therefore, it is important that organizations endorse positive compliance and introduce penalties for non-compliance as positive compliance behavior can minimize security incidents and increase ISP effectiveness (Humaidi & Balakrishnan, 2018; Parsons et al., 2015). There were no mentions of the penalties that would ensue if audits were failed or if surveys revealed there were issues that needed to be repaired. Results do show that institutions are doing their part to comply with state mandates and regulations. They also show that, even when not mandated, institutions are doing what they can, including promoting compliance, to prevent incidents.

The goal of GST is to methodically determine a system's inner workings such as subtleties, restrictions, conditions, and ideologies that can be distinguished and applied to systems on various levels. The hierarchy principle of GST relates to this theme down to the axiom that furthers it. The regulations sent down by the state are the objects treated as a whole and those regulations are made up of smaller objects (i.e. NIST, ISO, audits, etc.), which are to be regarded as wholes. The centrality axiom furthers this concept since the security strategies are built around the mandates and the implemented mandates themselves act as the sub-levels in the system. Business organizations, such as colleges and universities, are generally described as open systems when discussed in literature (Iwu et al., 2016). With open systems being malleable, it makes sense that different institutions have different means of protecting against intrusions. A vast number of protection efforts are proper for an open system.

It was very difficult to locate peer-reviewed documentation that discussed the state mandates within the university. With that, it is important to note that the research that was found extended the information gathered in this study. The NIST framework has achieved common use in some sectors in the U.S., with the U.S. Government using its purchasing authority to oblige higher education institutions to implement a NIST-based approach (Greene, 2019). Research identifies NIST, along with the CIS Controls identified by some participants, as cyber security best practices (Aliyu et al., 2020). The research conducted by Weidman and Grossklags (2018) found that 40% of all universities participating in their study referenced state and federal laws, or guidelines, along with links to HIPAA requirements or NIST standards. In this study, 60% of the participants referenced state regulations and 73.3% referenced NIST. HIPAA references came from 73.3% of participants, which will be discussed in the next section. New literature also shows that organizations need to successfully conduct IT audits to ensure suitable cyber security coverage (Stafford et al., 2018). This study stands to extend knowledge in the industry by

providing more of an insight into how state mandates play a role in college and university information security strategy and policy implementation.

Theme 5: SETA

The fifth and final emergent theme from the collected data was the implementation of a SETA program as a security strategy. Implementing a SETA program is important because humans have been identified in many studies as the weakest link in a security program. To properly protect PII, it is not enough to just have an InfoSec program in place. There must also be a plan in place to educate the individuals that are going to contribute to, monitor, maintain, and/or enforce the InfoSec program. During this study, user training, whether general or specific (i.e., HIPAA, FERPA, PCI), was listed as an essential facet to an effective InfoSec program.

The previous themes are chock-full of reasons for amending university security strategies. The question surrounding security strategy amendments elicited responses from 26.7% of the participants that indicated user training, an element of SETA, as a reason for modification. Participants 8 and 11 did not identify a SETA program but did use the incidents at other universities to educate employees at the institution. Participant 15 stated that the focus should be on end user training which leads to the next element of this theme which is derived from the question enquiring about the methods for measuring effectiveness. Twenty percent of the participants spoke about how user training success was considered when measuring effectiveness. Participants 2 and 10 measure the level of training completed by their users. Particularly for Participant 10's institution, attending the security awareness training tracks effectiveness by showing how well the participants scored. Anyone that does not achieve a sufficient score is forced to take the training over again. All employees are required to pass the security training.

Almost three quarters, or 73.3%, of the participants identified elements of SETA as the most beneficial security strategies. This backs up the research completed during the literature review that touted SETA programs as essential to a comprehensive ISP. Participant 11 implemented an official, formal training program. As security is everyone's job and helping users understand that concept is difficult, but not impossible. Participants 2 and 5 labeled security awareness as the foundation of their programs, while Participant 10 used security awareness training to educate its users on phishing emails. All the participants that identified user training as the most beneficial security strategy had various ways of completing their training, but all agreed that it was vital.

The final element of this theme came from the answer to the question asking what training is given to data custodians to aid in ensuring proper data security. Seven different codes surfaced when analyzing the data from this interview question. Only two of the participants explicitly mentioned SETA as a training concept. The other codes were fractions of a solid SETA program. Eighty-seven percent of the participants claimed that they have imparted at least a general form of training for data custodians. Participant 13 and Participant 8 make all new employees view a presentation on data security during their new employee orientation. Participant 9 provides special training to system administrators on how to run vulnerability scans. Each data custodian, due to their subject matter expertise in their area, has regulatory and other trainings that are required for their job and for data security at Participants 15 and 11's institutions. HIPAA and PCI training, respectively, were identified by 33.3% of the participants. There was a compliance committee instated that oversaw decisions about whether or not a specific technology or application can even be used at Participant 9's university in light of HIPAA compliance. Their institution is considered a covered entity under HIPAA compliance, so employees there are required to complete both HIPAA privacy training and HIPAA security

training on an annual basis. The employees that work in Participant 9's PCI environment are required to complete specialized training along with the institution's general security awareness training, which is required bi-annually. Participants 1 and 10 also require specialized PCI training at their universities.

FERPA, GLBA, and basic industry standards are the remaining training elements identified by the first interview question. Twenty-seven percent of the participants stated that their employees were to complete FERPA training. Annual FERPA training is given to the data custodians at Participant 7's institution. The training is disseminated within each department. Academic data handling is a requirement for FERPA training at the university of Participant 1. GLBA, first defined and mentioned in theme 4, was listed as one of the trainings issued to employees at the university of Participants 3 and 13. There was not much elaboration on the training, but it was noted that GLBA was a recent federal law the institution was obligated to abide by. Participants 12 and 14 noted some outside conferences and industry certifications that users can attend or obtain as training indicators. Participant 12 had a unique requirement of their employees by mandating the Security+ certification as a requirement for hire.

The literature review points out many of different elements to consider when looking into SETA. Flowerday and Tuyikeze (2016) conducted a study that indicated that the role of stakeholders and SETA were among the variables they deemed important for proper policy implementation. One of the tenants of InfoSec maintenance is adequate education, training, and awareness of security protocols. As this study, and others, have pointed out, one of the largest primary concerns when referencing InfoSec are the humans that interact with the system (Bauer, Bernroider, & Chudzikowski, 2017; Soomro, Shah, & Ahmed, 2016). People have been pinpointed as a weak link, thus making an ISP and a SETA program within an organization

imperative (Bauer, Bernroider, & Chudzikowski, 2017; Soomro, Shah, & Ahmed, 2016). It is projected that between 50% and 90% of security breaches are a result of human error in some fashion (Budzak, 2016). With proper SETA in place at universities, this number has the capability of shrinking within the higher education sector. Continuous, evolving training of all calibers of users across all types of data can be used as a preventative measure.

SETA is arguably the foundation of a solid InfoSec program. Systems-based approaches when referring to complex situations involving decision making enables the decision makers to address the situation fully (Yurtseven & Buchanan, 2016). Although this study most apparently relates to the systems technology aspect of GST, there is a portion of this study that relates very closely to systems philosophy. Protecting data is very complex as different threats surface regularly causing organizations, namely universities, to adapt almost immediately to avoid any issues. A university's approach to SETA can vary from university to university, region to region, and even country to country. There is thought that must go into how to best train the weakest link in data security. This theme, just like the other themes, also relates to the hierarchy approach as SETA is a whole concept that must be broken down into its individual parts, which are wholes in themselves.

There is plenty of new literature published that supports various SETA tactics to strengthen the weak link in data security. Research within the industry suggests that InfoSec misuses can be reduced by using SETA programs and computer monitoring as security countermeasures (Koohang, Anderson, Nord, & Paliszkiewicz, 2019). Security awareness training is stated to be the most economical method of security control (Koohang et al., 2019). It was also revealed that awareness programs reduced security threats and that there is a positive relationship amongst users' InfoSec awareness programs and their observed security efficiency

(Koohang et al., 2019). Hina, Selvam, and Lowry (2019) listed legal policy documents based on international standards, well planned SETA programs, and regular monitoring as commodities that would lead institutions toward the development of a comprehensive InfoSec culture. With higher education institutions experiencing the same threat and vulnerabilities as other business organizations, a lack of policy guidelines, lack of awareness of InfoSec dangers, and irregular monitoring of misuse behavior frequently lead to menacing situations (Hina & Dominic, 2020).

Applications to Professional Practice

The findings from this study provide a means for university data custodians to reduce the number of data breaches by successfully implementing a comprehensive information security strategy. University data custodians may discover value in these findings as there are an increasing number of university data incidents. The findings in this study may contribute to the improvement of IT practice by providing university data custodians with means of establishing a baseline strategy for securing millions of student, staff, and stakeholder records. These findings may also contribute to the non-educational sector as well, being that the strategies implemented are not specific for a given sector. When this study began, Privacy Rights Clearinghouse (2018), a non-profit that has been tracking and disseminating data breach statistics since 2005, was the organization that verified that eight of the 17 colleges and universities I applied to had been a victim of a data breach. Privacy Rights Clearinghouse (2020) also verified that over 11 billion records have been breached across all sectors between 2005 and 2020. An important aspect of this study is that it examined IT strategies that should be tailored for any IT professional to aid in the protection of PII so that another 11 billion records are not compromised.

Implications for Social Change

The findings from this study may impact social change by reducing duplicitous use of PII obtained maliciously from colleges and universities. Staff, students, and other stakeholder information discovered by a data breach can have a significant negative impact on higher education institutions and everyone that is involved. Implementing comprehensive information security strategies might affect how university data custodians protect university data by providing an efficient barrier to further thwart attacks from the outside and within. The quantity and severity of data breaches at higher education institutions are incessantly increasing due to low InfoSec awareness levels, employee negligence, lost or stolen devices, social media, mischievous website attacks, unintentional disclosure of sensitive information, viruses/malware, and insecure third-party email attachments (Hina et al., 2019). Understanding, implementing, and monitoring the necessary components that make a comprehensive information security strategy can address each of these areas, which, as shown in this study, is imperative for establishing a thriving InfoSec culture.

Another social implication is attentiveness to the need for financial and personnel resources. There were a disproportionate number of participants that indicated concern about budget for the institution and how it directly impacted not only their ability to carry out their jobs daily, but also how it impacted hiring personnel to do the jobs requested, having enough personnel to divide amongst the tasks present, and the ability to execute requirements to implement state mandates. With leadership now having more knowledge about inner-institutional concerns and seeing how the participants have been directly impacted by their governing bodies decision to cut, shift, or underfund when developing the budget for a vital piece of society, it is with high hopes that this information dissuades leadership from making the same mistake. The

goal is to bring awareness and hopefully give the institutions the resources they need to protect data.

The final social implication refers to an underlying issue with personnel in cyber security. While conducting the interviews and gathering data, it was discovered that there was not only an issue with the budget to attract, hire, and keep personnel, but there was also an issue with finding qualified personnel. An (ISC) 2 Cyber Security Workforce study publicized that there is a shortage of about three million cyber security professionals globally and the issues associated with the workforce shortage have only become more prominent (Kam et al., 2020). As stated before, when there is a lack of knowledgeable personnel applying InfoSec defenses, organizational information resources will be vulnerable to cyber-attacks (Kam, 2020). The goal of this study was to identify the information security strategies that university data custodians use to protect PII collected from staff, students, and other stakeholders. Using SETA, an identified security strategy indicated as one of the most beneficial, to educate youth of diverse backgrounds would assist with alleviating the critical shortage identified in the reference. It would also diversify to the information security strategies that are administered within these institutions. With the critical shortage of cyber security talent, InfoSec experts and scholars should embolden cyber security skills within novices and encourage them to pursue cyber security education (Kam, 2020). This, in turn, would give university data custodians a larger pool of eligible candidates from which to choose. There would also be less concern about the eligibility of the youth if it is known that they were educated by the university pipeline at an early age.

Recommendations for Action

University data custodians should implement, promote, and monitor comprehensive information security strategies to protect university PII. University data custodians. IT leadership

of all levels, state legislators, and individuals that have an interest in moving into the cyber security space in higher education should take heed to these recommendations. Prior to doing anything, the budget should be confirmed, and all necessary training should be disseminated. This provides a foundation for the plan as proper personnel and sufficient resources are confirmed.

After the required resources have been confirmed, data custodians need to develop an action plan so that progress can be measured, and nothing is overlooked while completing the process. This action plan should state a timetable, a measurement to be used to determine effectiveness, who is responsible for which actions, and what method will be used to maintain and monitor the security strategies once they are implemented. Once the plan is developed, it should be reviewed and refined with the entire IT team to make sure that all areas are covered and that the proper personnel is available to take care of the assigned tasks. Senior IT leadership should then prep the IT team for implementation. This shows that leadership has bought into the plan and is invested in its success. After the strategies are implemented, an evaluation must commence. This evaluation should consist of discovering what went well and what could have gone better. It should also make sure that all goals were met and what, if any, improvements need to be made. This is where the assessments and audits fit in the plan. If any improvements are needed, there should be a plan put in place to make the corrections. Plans make it easier to track if goals are met as well as the portion of the process that could have caused any issues that may present themselves. The final step in this process is to communicate and normalize the implemented security strategies. This is the part of the process where users are trained and engaged. It is important to set the expectations for frequency of training, how the training will be administered, and who the points of contact are in case of questions or concerns.

All these subgroups will have access to the results of this study as it will be published. I will also create an abbreviated version of this study to publish in peer-reviewed journals. Further research will be done on various segments of this study to provide additional, up-to-date information on the pressing topics that could alter the state of cyber security. Publication of this research will also be publicized on various social media platforms once it is approved.

Recommendations for Further Study

Data custodians collect, manage, and store data collected for various reasons and would be held accountable for data distribution (Smith et al., 2015). They would also be held accountable for data disruption as well. To further this study and assist data custodians in preventing data disruption, the elements of the themes should be further investigated to gain more specific information and perspective. An examination of the plans that are developed prior to implementation is also a suggestion. Discovering a means of producing enough individuals to fill that three-million-person gap in cyber security is also going to be imperative.

One of the limitations of this study was that the participants targeted may not have the breadth of knowledge needed to give adequate information. Although data custodians are professionals, with their levels of knowledge not being researched, there was no way to determine the actual amount of knowledge the participant had about their position. Using participants that have a predetermined number of consecutive years in their position or at their university could address this limitation. The other limitation of this study was that the study findings may not have been generalized for all the U.S. since the case study focused on institutions of higher education in the Carolinas. Conducting this study for each region, state, and/or territory in the U.S., and disseminating it as a reflection of the nation could address this limitation.

Reflections

Being a career student for 15 years, this was admittedly the most strenuous, stressful, time consuming, yet rewarding process ever attempted. As someone that has been a victim of several data breaches, as well as a person that has been responsible for assisting with the prevention of a breach, this topic was real and relevant. While being both the victim and the data custodian, the presence of personal bias was inevitable. This bias was, however, reduced by understand the bias and the steps to take to diminish any present bias. Relating to the participants as someone in the IT could have affected the participants. Explaining the importance of this topic and taking the time to speak with the participants understand their want and need for assistance with the issues they are facing daily also could have affected the participants. There is no change in thinking after completing this study, but there is a better understanding of how to formulate a study, how to solicit participants, and how to write up the data. These are all important aspects to understand as a researcher that wishes to go on and get published in peer-reviewed academic journals.

Summary and Study Conclusions

Comprehensive information security strategies, whether they consist of training, monitoring, new defensive technology, or all the above, are the founding blocks of an InfoSec program. Without these strategies, data custodians are defenseless against malicious attacks. IT leadership needs to provide resources for data custodians to do their jobs. Data custodians need to create plans to implement mandated and recommended security strategies. Users need training and exposure to these strategies so that they can do their part to protect data at the institution. Putting the data of staff, students, and other stakeholders at risk because of a lack of strategies

should not be accepted. Normalizing a positive InfoSec culture should be a mandate not only in higher education institutions, but in other organizations as well.

References

Adhabi, E., & Anozie, C. B. (2017). Literature review for the type of interview in qualitative research. *International Journal of Education, 9*(3), 86–97. doi:10.5296/ije.v9i3.11483

Ahmad, A., Malik, A. W., Alreshidi, A., Khan, W., & Sajjad, M. (2019). Adaptive security for self-protection of mobile computing devices. *Mobile Networks and Applications*, 1–20. doi:10.1007/s11036-019-01355-y

Akçayır, M., & Akçayır, G. (2017). Advantages and challenges associated with augmented reality for education: A systematic review of the literature. *Educational Research Review, 20,* 1–11. doi:10.1016/j.edurev.2016.11.002

Akram, R. N., & Ko, R. K. (2014). Unified model for data security - A position paper. *2014 IEEE 13Th International Conference on Trust, Security & Privacy in Computing & Communications*, 831. doi:10.1109/TrustCom.2014.110

Ali, S. N. M., Mokhtar, S., Noor, A. M., Johari, N., Fauzi, N. S., & Salleh, N. A. (2018). A study on integration of Waqf Real Estate and Zakat: A qualitative investigation for Asnaf Muallafs' welfare. In *IOP Conference Series: Earth and Environmental Science, 117*(1), 012021. IOP Publishing. doi:10.1088/1755-1315/117/1/012021

Aljumaili, M., Wandt, K., Karim, R., & Tretten, P. (2015). eMaintenance ontologies for data quality support. *Journal of Quality in Maintenance Engineering, 21*(3), 358–374. doi:10.1108/JQME-09-2014-0048

Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher

education institutions in the United Kingdom. *Applied Sciences, 10*(10), 3660. doi:10.3390/app10103660

Almalki, S. (2016). Integrating quantitative and qualitative data in mixed methods research--challenges and benefits. *Journal of Education and Learning, 5*(3), 288–296. doi:10.5539/jel.v5n3p288

Alqahtani, F. H. (2017). Developing an information security policy: A case study approach. *Procedia Computer Science, 124*, 691–697. doi:10.1016/j.procs.2017.12.206

Alshare, K. A., Lane, P. L., & Lane, M. R. (2018). Information security policy compliance: A higher education case study. *Information & Computer Security, 26*(1), 91–108. doi:10.1108/ICS-09-2016-0073

Alves, R. A., Limpo, T., Fidalgo, R., Carvalhais, L., Pereira, L. Á., & Castro, S. L. (2016). The impact of promoting transcription on early text production: Effects on bursts and pauses, levels of written language, and writing performance. *Journal of Educational Psychology, 108*(5), 665. doi:10.1037/edu0000089

Amankwaa, L. (2016). Creating protocols for trustworthiness in qualitative research. *Journal of Cultural Diversity, 23*(3), 121–127. Retrieved form https://www.ncbi.nlm.nih.gov/pubmed/29694754

Annink, A. (2017). Using the research journal during qualitative data collection in a cross-cultural context. *Entrepreneurship Research Journal, 7*(1). doi:10.1515/erj-2015-0063

Anton, N., & Nedelcu, A. (2015). The systemic approach to information protection in

relation to risk in an integrated information security system. *Applied Mechanics & Materials*, 760689. doi:10.4028/www.scientific.net/AMM.760.689

Astakhova, L. V. (2020). Issues of the culture of information security under the conditions of the digital economy. *Scientific and Technical Information Processing*, *47*, 56–64. doi:10.3103/s0147688220010062

Axelsson, J. (2019). Game theory applications in systems-of-systems engineering: A literature review and synthesis. *Procedia Computer Science*, *153*(1), 154–165. doi:10.1016/j.procs.2019.05.066

Azevedo, V., Carvalho, M., Fernandes-Costa, F., Mesquita, S., Soares, J., Teixeira, F., & Maia, Â. (2017). Interview transcription: Conceptual issues, practical guidelines, and challenges. *Revista de Enfermagem Referência, 4*(14), 159–167. doi:10.12707/RIV17018

Bauer, S., Bernroider, E. W. N., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security*, *68*, 145–159. doi:10.1016/j.cose.2017.04.009

Beaudin, K. (2015). College and university data breaches: Regulating higher education cybersecurity under state and federal law. *JC & UL, 41*, 657. Retrieved from https://heinonline.org/HOLP/P?h=hein.journals/jcolunly41&i=691

Beebe, S. N. (2004). A changing society-perceptions of health needs for non-metropolitan seniors and baby boomers in retirement. *Californian Journal of Health Promotion, 2*(3), 67–81. Retrieved from

http://www.cjhp.org/Volume2_2004/Issue3/67-81-beebe.pdf

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior, 48*, 51–61. doi:10.1016/j.chb.2015.01.039

Bergstrom, J., van Winsen, R., & Henriqson, E. (2015). On the rationale of resilience in the domain of safety: A literature review. *Reliability Engineering & System Safety, 141,* 131–141. doi:10.1016/j.ress.2015.03.008

Binkley, J. W. (2016). Fair notice of unfair practices: Due process in FTC data security enforcement after Wyndham. *Berkeley Technology Law Journal, 31*(2), 1079–1108. doi:10.15779/Z389857

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation?. *Qualitative Health Research, 26*(13), 1802–1811. doi:10.1177/1049732316654870

Blagden, N., & Perrin, C. (2018). The impact of a brief structured intervention on young offenders masculine identity: A mixed methods study. *Journal of criminal psychology, 8*(3), 173–186. doi:10.1108/JCP-11-2017-0042

Bolderston, A. (2012). Conducting a research interview. *Journal of Medical Imaging and Radiation Sciences, 43*(1), 66–76. doi:10.1016/j.jmir.2011.12.002

Boone, A. (2017). Cyber-security must be a C-suite priority. *Computer Fraud & Security, 2017*(2), 13–15. doi:10.1016/S1361-3723(17)30015-5

Broman, K. W., & Woo, K. H. (2018). Data organization in spreadsheets. *The American Statistician, 72*(1), 2–10. doi:10.1080/00031305.2017.1375989

Brown, H. S. (2016). After the data breach: Managing the crisis and mitigating the impact. *Journal of business continuity & emergency planning, 9*(4), 317–328. Retrieved from https://www.ncbi.nlm.nih.gov/pubmed/27318286

Browne, E. L. (2018). Black virgin islands male high school dropouts: A qualitative study. *The Qualitative Report, 23*(8), 1932–1947. Retrieved from https://search.proquest.com/docview/2231815967?accountid=10504

Budzak, D. (2016). Information security–The people issue. *Business Information Review, 33*, 85–89. doi:10.1177/0266382116650792

Burley, S., Cox, R., di Tommaso, A., & Molineux, M. (2018). Primary contact occupational therapy hand clinics: The pull of an occupational perspective. *Australian Occupational Therapy Journal, 65*(6), 533–543. doi:10.1111/1440-1630.12507

Cafarella, B. (2016). Acceleration and compression in developmental mathematics: Faculty viewpoints. *Journal of Developmental Education, 39*(2), 12. Retrieved from https://eric.ed.gov/?id=EJ1117729

Call-Cummings, M., Dennis, B., & Martinez, S. (2019). The role of researcher in participatory inquiry: Modeling intra-active reflexivity in conversational reflections. *Cultural Studies ↔ Critical Methodologies, 19*(1), 68–76. doi:10.1177/1532708617750677

Candela, A. G. (2019). Exploring the function of member checking. *The Qualitative Report, 24*(3), 619–628. Retrieved from https://nsuworks.nova.edu/tqr/vol24/iss3/14

Capina, A. B., & Bryan, G. (2017). Engaging reluctant readers in a French immersion classroom. *Current Issues in Education, 20*(1), 1–22. Retrieved from https://cie.asu.edu/ojs/index.php/cieatasu/article/view/1642

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *The Qualitative Report, 21*(5), 811–831. Retrieved from http://nsuworks.nova.edu/tqr/vol21/iss5/2

Caws, P. (2015). General systems theory: Its past and potential. *Systems Research and Behavioral Science, 32*(5), 514–521. doi:10.1002/sres.2353

Cease, C. C. (2014). Giving out your number: A look at the current state of data breach litigation. *Ala. L. Rev., 66*(2), 395–422. Retrieved from https://heinonline.org/HOL/P?h=hein.journals/bamalr66&i=415

Ceric, A. (2015). Bringing together evaluation and management of ICT value: A systems theory approach. *The Electronic Journal of Information Systems Evaluation, 18*(1), 19–35. Retrieved from http://www.ejise.com/main.html

Chatterjee, S., Xiao, X., Elbanna, A., & Saker, S. (2017). The information systems artifact: A conceptualization based on general systems theory. In *Proceedings of the 50th Hawaii International Conference on System Sciences*, 5717–5726. Retrieved from http://hdl.handle.net/10125/41852

Chauvette, A., Schick-Makaroff, K., & Molzahn, A. E. (2019). Open Data in Qualitative Research. *International Journal of Qualitative Methods, 18*(1), 1–6. doi:10.1177/1609406918823863

Chen, H. T. (2016). Interfacing theories of program with theories of evaluation for

advancing evaluation practice: Reductionism, systems thinking, and pragmatic synthesis. *Evaluation and program planning, 59*(1), 109–118. doi:10.1016/j.evalprogplan.2016.05.012

Chen, X., Wu, D., Chen, L., & Teng, J. K. L. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management, 55*(1), 1049–1060. doi:10.1016/j.im.2018.05.011

Choi, S., Martins, J. T., & Bernik, I. (2018). Information security: Listening to the perspective of organisational insiders. *Journal of Information Science, 44*(6), 752–767. doi:10.1177/0165551517748288

Chung, M. (2020). Signs your cyber security is doomed to fail. *Computer Fraud & Security*, *2020*(3), 10–13. doi:10.1016/S1361-3723(20)30029-4

Clark, R., & McLean, C. (2018). The professional and personal debriefing needs of ward based nurses after involvement in a cardiac arrest: An explorative qualitative pilot study. Intensive and Critical Care Nursing, *47*, 78–84. doi:10.1016/j.iccn.2018.03.009

Clarke, D. E., Boyce-Gaudreau, K., Sanderson, A., & Baker, J. A. (2015). ED triage decision-making with mental health presentations: A "think aloud" study. *Journal Of Emergency Nursing, 41*(6), 496–502. doi:10.1016/j.iccn.2018.03.009

Connelly, L. M. (2016). Trustworthiness in qualitative research. *Medsurg Nursing, 25*(6), 435–437. Retrieved from https://www.ncbi.nlm.nih.gov/pubmed/30304614

Daniel, P. A., & Daniel, C. (2018). Complexity, uncertainty and mental models: From a

paradigm of regulation to a paradigm of emergence in project management. *International Journal of Project Management, 36*(1), 184–197. doi:10.1016/j.ijproman.2017.07.004

da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Information & Computer Security, 24*(2), 139–151. doi:10.1108/ICS-12-2015-0048

Dean, J. (2014). Personal protective equipment: An antecedant to safe behavior? *Professional Safety, 59*(2), 41–46. Retrieved from https://search.proquest.com/docview/1517909674?pq-origsite=gscholar

Dempsey, L., Dowling, M., Larkin, P., & Murphy, K. (2016). Sensitive interviewing in qualitative research. *Research In Nursing & Health, 39*(6), 480–490. doi:10.1002/nur.21743

Densham, B. (2015). Three cyber-security strategies to mitigate the impact of a data breach. *Network Security*, *2015*(1), 5–8. doi:10.1016/S1353-4858(15)70007-3

Diaz, L. J., Anderson, M. C., Wolak, J. T., & Opderbeck, D. (2017). The Risks and Liability of Governing Board Members to Address Cyber Security Risks in Higher Education. *JC & UL, 43*(1), 49–76. Retrieved from https://heinonline.org/HOL/P?h=hein.journals/jcolunly43&i=55

Dikko, M. (2016). Establishing construct validity and reliability: Pilot testing of a qualitative interview for research in Takaful (Islamic insurance). *The Qualitative Report, 21*(3), 521–528. Retrieved from http://nsuworks.nova.edu/tqr/vol21/iss3/6

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management, 29*(6), 449–457. doi:10.1016/j.ijinfomgt.2009.05.003

Drack, M., & Pouvreau, D. (2015). On the history of Ludwig von Bertalanffy's "General Systemology", and on its relationship to cybernetics – part III: Convergences and divergences. *International Journal of General Systems, 44*(5), 523–571. doi:10.1080/03081079.2014.1000642

du Pisani, K. (2018). Father of holism: Was Jan Smuts an intellectual? *Tydskrif Vir Geesteswetenskappe, 58*(1), 1–16. doi:10.17159/2224-7912/2018/v58n1a1

Elhai, J. D., & Hall, B. J. (2015). How secure is mental health providers' electronic patient communication? An empirical investigation. *Professional Psychology: Research and Practice, 46*(6), 444–450. doi:10.1037/pro0000054

Farcasin, M., & Chan-tin, E. (2015). Why we hate IT: two surveys on pre-generated and expiring passwords in an academic setting. *Security and Communication Networks, 8*(13), 2361–2373. doi:10.1002/sec.1184

Fazlida, M. R., & Said, J. (2015). Information Security: Risk, Governance and Implementation Setback. *Procedia Economics and Finance, 28*(1), 243–248. doi:10.1016/S2212-5671(15)01106-5

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security, 61*(C), 169–183. doi:10.1016/j.cose.2016.06.002

Fontainha, T. C., Leiras, A., de Mello Bandeira, R. A., & Scavarda, L. F. (2017). Public-private-people relationship stakeholder model for disaster and humanitarian operations. *International Journal of Disaster Risk Reduction*, 22, 371–386. doi:10.1016/j.ijdrr.2017.02.004

Furman, S. M., Theofanos, M. F., Choong, Y., & Stanton, B. (2012). Basing Cybersecurity Training on User Perceptions. *Security & Privacy, IEEE, 10*(2), 40–49. doi:10.1109/MSP.2011.180

Fusch, P., Fusch, G. E., & Ness, L. R. (2018). Denzin's Paradigm Shift: Revisiting Triangulation in Qualitative Research. *Journal of Social Change, 10*(1), 19–32. doi:10.5590/JOSC.2018.10.1.02

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report, 20*(9), 1408–1416. Retrieved from https://nsuworks.nova.edu/tqr/vol20/iss9/3/

Gentles, S. J., Charles, C., Ploeg, J., & McKibbon, K. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *The Qualitative Report, 20*(11), 1772–1789. Retrieved from https://nsuworks.nova.edu/tqr/vol20/iss11/5

Gesch-Karamanlidis, E. (2015). Reflecting on novice qualitative interviewer mistakes. *The Qualitative Report, 20*(5), 712–726. Retrieved from https://nsuworks.nova.edu/tqr/vol20/iss5/12

Gill, P., & Baillie, J. (2018). Interviews and focus groups in qualitative research: an update for the digital age. *British Dental Journal, 225*(7), 668–672.

doi:10.1038/sj.bdj.2018.815

Gous, J. G., Eloff, I., & Moen, M. C. (2014). How inclusive education is understood by principals of independent schools. *International Journal of Inclusive Education, 18*(5), 535–552. doi:10.1080/13603116.2013.802024

Grabosky, P. (2018). Sympathy for the devil: State engagement with criminal organisations in furtherance of public policy. *International Journal of Comparative and Applied Criminal Justice, 43*(3), 1–17. doi:101080/01924036.2018.1543129

Graham, A., Powell, M. A., & Taylor, N. (2015). Ethical research involving children: Encouraging reflexive engagement in research with children and young people. *Children & Society, 29*(5), 331–343. doi:10.1111/chso.12089

Greene, F.P (2019). Managing the hypercomplexity of cyber security regulation: In search of a regulatory Rosetta Stone. *Cyber Security: A Peer-Reviewed Journal*, 3(2), 134–144. Retrieved from https://www.hselaw.com/files/Greene_May_2019.pdf

Groenewald, T. (2004). A phenomenological research design illustrated. *International Journal of Qualitative Methods, 3*(1), 42–55. doi:10.1177/160940690400300104

Guest, G., Namey, E., Taylor, J., Eley, N., & McKenna, K. (2017). Comparing focus groups and individual interviews: findings from a randomized study. *International Journal of Social Research Methodology, 20*(6), 693–708. doi:10.1080/13645579.2017.1281601

Gwebu, K. L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis

response strategies in data breach management. *Journal of Management Information Systems, 35*(2), 683–714. doi:10.1080/07421222.2018.1451962

Hadi, M. A., & Closs, S. J. (2016). Ensuring rigour and trustworthiness of qualitative research in clinical pharmacy. *International journal of clinical pharmacy, 38*(3), 641–646. doi:10.1007/s11096-015-0237-6

Halcomb, E., & Hickman, L. (2015). Mixed methods research. *Nursing Standard, 29*(32), 41–47. doi:10.7748/ns.29.32.41.e8858

Han, J., Kim, Y. J., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers and Security, 66*(C), 52–65. doi:10.1016/j.cose.2016.12.016

Hayashi, P., Jr., Abib, G., & Hoppen, N. (2019). Validity in qualitative research: A processual approach. *The Qualitative Report, 24*(1), 98–112. Retrieved from https://nsuworks.nova.edu/tqr/vol24/iss1/8

Haydn, T. (2019). Triangulation in history education research, and its limitations: A view from the UK. *History Education Research Journal, 16*(1), 35–49. doi:10.18546/HERJ.16.1.04

Hemphill, T. A., & Longstreet, P. (2016). Financial data breaches in the US retail economy: Restoring confidence in information technology security standards. *Technology in Society, 44*(C), 30–38. doi:10.1016/j.techsoc.2015.11.007

Herrmann, J. (2017). Experiences, challenges, and lessons learned—Interviewing Rwandan survivors of sexual violence. *Griffith Journal of Law & Human Dignity, 5*(1), 165–188. Retrieved from

https://griffithlawjournal.org/index.php/gjlhd/article/view/892

Hina, S., & Dominic, P. D. D. (2020). Information security policies' compliance: A perspective for higher education institutions. *Journal of Computer Information Systems*, *60*(3), 201–211. doi:10.1080/08874417.2018.1432996

Hina, S., Selvam, D. D. D. P., & Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers & Security*, *87*, 101594. doi:10.1016/j.cose.2019.101594

Horne, C. A., Maynard, S. B., & Ahmad, A. (2017). Organisational information security strategy: Review, discussion and future research. *Australasian Journal of Information Systems, 21,* 1–17. doi:10.3127/ajis.v21i0.1427

Hovav, A., & Putri, F. F. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing, 32*(C), 35–49. doi:10.1016/j.pmcj.2016.06.007

Hughes, B. P., Newstead, S., Anund, A., Shu, C. C., & Falkmer, T. (2015). A review of models relevant to road safety. *Accident Analysis and Prevention, 74*, 250–270. doi:10.1016/j.aap.2014.06.003

Humaidi, N., & Balakrishnan, V. (2018). Indirect effect of management support on users' compliance behaviour towards information security policies. *Health Information Management: Journal Of The Health Information Management Association Of Australia*, *47*(1), 17–27. doi:10.1177/1833358317700255

Iannuzzi, D., Grant, A., Corriveau, H., Boissy, P., & Michaud, F. (2016). Specification of

an integrated information architecture for a mobile teleoperated robot for home telecare. *Informatics for Health and Social Care, 41*(4), 350–361. doi:10.3109/17538157.2015.1033527

Ibor, A. E., & Obidinnu, J. N. (2015). System hardening architecture for safer access to critical business data. *Nigerian Journal Of Technology, 34*(4), 788–792. doi:10.4314/njt.v34i4.17

Inoue, J. I., Ghosh, A., Chatterjee, A., & Chakrabarti, B. K. (2015). Measuring social inequality with quantitative methodology: Analytical estimates and empirical data analysis by gini and k indices. *Physica A: Statistical Mechanics and its Applications*, 429, 184–204. doi:10.1016/j.physa.2015.01.082

Iwu, C. G., Kapondoro, L., Twum-Darko, M., & Lose, T. (2016). Strategic human resource metrics: A perspective of the general systems theory. *Acta Universitatis Danubius: Oeconomica, 12*(2), 5. Retrieved from http://journals.univ-danubius.ro/index.php/oeconomica/article/view/3191

Jokela, P., Karlsudd, P., & Östlund, M. (2008). Theory, method and tools for evaluation using a systems-based approach. *Electronic Journal Of Information Systems Evaluation, 11*(3), 197–212. Retrieved from http://www.ejise.com/volume11/issue3/p139

Joshi, C., & Singh, U. K. (2017). Information security risks management framework – A step towards mitigating security risks in university network. *Journal of Information Security and Applications, 35*(C), 128–137. doi:10.1016/j.jisa.2017.06.006

Kallio, H., Pietilä, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal Of Advanced Nursing, 72*(12), 2954–2965. doi:10.1111/jan.13031

Kam, H. J., Menard, P., Ormond, D., & Crossler, R. E. (2020). Cultivating cybersecurity learning: An integration of self-determination and flow. *Computers & Security*, 101875. doi:10.1016/j.cose.2020.101875

Keating, C. B., Katina, P. F., Bradley, J. M., & Pyne, J. C. (2016). Systems theory as a conceptual foundation for system of systems engineering. *INSIGHT, 19*(3), 47–50. doi:10.1002/inst.12108

Kesić, S. (2016). Systems biology, emergence and antireductionism. *Saudi Journal Of Biological Sciences, 23*(5), 584–591. doi:10.1016/j.sjbs.2015.06.015

Khorana, S., Ferguson-Boucher, K., & Kerr, W. A. (2015). Governance issues in the EU's e-procurement framework. *JCMS: Journal of Common Market Studies, 53*(2), 292–310. doi:10.1111/jcms.12179

Kinchin, G., Ismail, N., & Edwards, J. A. (2018). Pilot study, Does it really matter? Learning lessons from conducting a pilot study for a qualitative PhD thesis. *International Journal of Social Science Research, 6*(1), 1–17. doi:10.5296/ijssr.v6i1.11720

Koerber, A., & McMichael, L. (2008). Qualitative sampling methods: A primer for technical communicators. *Journal Of Business And Technical Communication, 22*(4), 454–473. doi:10.1177/1050651908320362

Koohang, A., Anderson, J., Nord, J. H., & Paliszkiewicz, J. (2019). Building an awareness-centered information security policy compliance model. Industrial Management & Data Systems. doi:10.1108/IMDS-07-2019-0412

Kordova, S., Frank, M., & Miller, A. (2018). Systems thinking education—Seeing the forest through the trees. *Systems, 6*(3), 29–43. doi:10.3390/systems6030029

Krupic, F., Eisler, T., Sköldenberg, O., & Fatahi, N. (2016). Experience of anaesthesia nurses of perioperative communication in hip fracture patients with dementia. *Scandinavian Journal Of Caring Sciences, 30*(1), 99–107. doi:10.1111/scs.12226

Kuper, A., Lingard, L., & Levinson, W. (2008). Critically appraising qualitative research. *BMJ*, 337(a1035), 687–689. doi:10.1136/bmj.a1035

Lancaster, K. (2017). Confidentiality, anonymity and power relations in elite interviewing: Conducting qualitative policy research in a politicised domain. *International Journal of Social Research Methodology, 20*(1), 93–103. doi:10.1080/13645579.2015.1123555

Lanclos, D., & Asher, A. D. (2016). 'Ethnographish': The state of the ethnography in libraries. *Weave: Journal of Library User Experience, 1*(5). doi:10.3998/weave.12535642.0001.503

Leung, Y. K., Leung, Y. W., & Yuen, T. W. W. (2016). The contribution of advocacy NGOs in governance through cultivating of a participatory culture: Case studies in Hong Kong. *Universal Journal of Educational Research, 4*(3), 490–500. doi:10.13189/ujer.2016.040304

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five

approaches. *Health Promotion Practice, 16*(4), 473–475. doi:10.1177/1524839915580941

Liao, H., & Hitchcock, J. (2018). Reported credibility techniques in higher education evaluation studies that use qualitative methods: A research synthesis. *Evaluation and Program Planning, 68*(C), 157–165. doi:10.1016/j.evalprogplan.2018.03.005

Limakrisna, N., & Ali, H. (2016). Model of customer satisfaction: Empirical study at fast food restaurants in bandung. *International Journal of Business and Commerce, 5*(6), 132–146. Retrieved from https://www.ijbcnet.com/5-6/IJBC-16-5615.pdf

Lorio, P. J. (2017). Access denied: Data breach litigation, article III standing, and a proposed statutory solution. *Colum. JL & Soc. Probs., 51*(1), 79–128. doi:10.2139/ssrn.2996533

Lugo, R. G., Firth-Clark, A., Knox, B. J., Jøsok, Ø., Helkala, K., & Sütterlin, S. (2019). Cognitive profiles and education of female cyber defence operators. *International Conference on Human-Computer Interaction*, 563–572. doi:10.1007/978-3-030-22419-6_40

Mahanani, W. (2018). The influence of collective action, community empowerment, and shared vision to the community capacity in urban water resource conservation. *IOP Conference Series: Earth and Environmental Science, 200*(1), 012040. IOP Publishing. doi:10.1088/1755-1315/200/1/012040

Mahmoud, E., Seyed, S., & Hon, C. (2016). The internet of things: New interoperability, management and security challenges. *International Journal of Network Security & Its Applications, 8*(2), 85–102. doi:10.5121/ijnsa.2016.8206

Malecic, A. (2017). Footprints of General Systems Theory. *Systems Research and Behavioral Science*, *34*(5), 631–636. doi:10.1002/sres.2484

Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative interview studies: Guided by information power. *Qualitative Health Research*, *26*(13), 1753–1760. doi:10.1177/1049732315617444

Manners, B., Kruger, M., & Saayman, M. (2016). Managing live music performances: A demand and supply analysis. *Event Management*, *20*(2), 147–163. doi:10.3727/152599516X14610017108620

Mäntykangas, A. A. M. s. (2018). Information security issues in higher education. *ELearning & Software for Education*, *4*(14), 378–381. doi:10.12753/2066-026X-18-267

McCormack, L., & Thomson, S. (2017). Complex trauma in childhood, a psychiatric diagnosis in adulthood: Making meaning of a double-edged phenomenon. *Psychological Trauma: Theory, Research, Practice, and Policy*, *9*(2), 156. doi:10.1037/tra0000193

McGrath, C., Palmgren, P. J., & Liljedahl, M. (2018). Twelve tips for conducting qualitative research interviews. *Medical Teacher*, 1–5. doi:10.1080/0142159X.2018.1497149

Mehrez, A. (2013). Investigating the role of knowledge gap in enhancing software quality. *Journal of Knowledge Management, Economics and Information Technology*, *3*(1). Retrieved from https://EconPapers.repec.org/RePEc:spp:jkmeit:1348

Miller, T. (2017). Telling the difficult things: Creating spaces for disclosure, rapport and 'collusion'in qualitative interviews. In *Women's Studies International Forum, 61*(C), 81–86. Pergamon. doi:10.1016/j.wsif.2016.07.005

Mingers, J. (2017). Back to the future: A critique of Demetis and Lee's "Crafting theory to satisfy the requirements of systems science". *Information and Organization, 27*(1), 67–71. doi:10.1016/j.infoandorg.2017.01.003

Miracle, V. A. (2016). The Belmont report: The triple crown of research ethics. *Dimensions of Critical Care Nursing, 35*(4), 223–228. doi:10.1097/DCC.0000000000000186

Misenheimer, K. J. (2016). Training users to be aware of computer and information security on college and university campuses. *Journal of Information Systems Technology & Planning, 8*(19), 61–75. Retrieved from https://mafiadoc.com/jistp-volume-8-issue-19_5b70b411097c47b8498b45bc.html

Mohajan, H. K. (2018). Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment and People, 7*(1), 23–48. doi:10.26458/jedep.v7i1.571

Montesdioca, G. P. Z., & Maçada, A. C. G. (2015). Measuring user satisfaction with information security practices. *Computers & Security, 48*(C), 267–280. doi:10.1016/j.cose.2014.10.015

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly, 42*(1), 285–311. doi:10.25300/MISQ/2018/13853

Morgan, D. L. (2018). Living within blurry boundaries: The value of distinguishing between qualitative and quantitative research. *Journal of Mixed Methods Research, 12*(3), 268–279. doi:10.1177/1558689816686433

Moser, A., & Korstjens, I. (2018). Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. *European Journal of General Practice, 24*(1), 9–18. doi:10.1080/13814788.2017.1375091

Natow, R. S. (2019). The use of triangulation in qualitative studies employing elite interviews. *Qualitative Research,* 1–14. doi:10.1177/1468794119830077

Ncube, C., & Garrison, C. P. (2010). Lessons learned from university data breaches. *Palmetto Business and Economic Review, 13*(2010), 27–37. doi:10.1.1.392.9280

Ndiege, J. R., & Okello, G. O. (2018). Information security awareness amongst students joining higher academic institutions in developing countries: Evidence from Kenya. *The African Journal of Information Systems, 10*(3), 4. Retrieved from http://erepo.usiu.ac.ke/11732/4329

Nottingham, S., & Mazerolle, S. M. (2018). Mentoring processes in higher education: perspectives of junior athletic training faculty members. *Internet Journal of Allied Health Sciences and Practice, 16*(4), 1. Retrieved from https://nsuworks.nova.edu/ijahsp/vol16/iss4/1/

Oesterreich, T. D., & Teuteberg, F. (2018). Looking at the big picture of IS investment appraisal through the lens of systems theory: A system dynamics approach for understanding the economic impact of BIM. *Computers in Industry, 99*(2018), 262–281. doi:10.1016/j.compind.2018.03.029

Oestreicher, C. (2007). A history of chaos theory. *Dialogues in Clinical Neuroscience, 9*(3), 279–289. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3202497/

Okanazu, O.O., Madu, M.A., Igboke, S. A. (2019). A recipe for efficient and corrupt free public sector. *Central European Journal of Labour Law and Personnel Management, 2*(1), 29–46. doi: 10.33382/cejllpm.2019.02.03

O'Keeffe, J., Buytaert, W., Mijic, A., Brozović, N., & Sinha, R. (2016). The use of semi-structured interviews for the characterisation of farmer irrigation practices. *Hydrology and Earth System Sciences, 20*(5), 1911–1924. doi:10.5194/hessd-12-8221-2015

Olifer, D., Goranin, N., Kaceniauskas, A., & Cenys, A. (2017). Controls-based approach for evaluation of information security standards implementation costs. *Technological and Economic Development of Economy, 23*(1), 196–219. doi:10.3846/20294913.2017.1280558

O'Neill, L., Dexter, F., & Zhang, N. (2016). The risks to patient privacy from publishing data from clinical anesthesia studies. *Anesthesia & Analgesia, 122*(6), 2017–2027. doi:10.1213/ANE.0000000000001331

Opderbeck, D. W. (2015). Current developments in data breach litigation: Article III standing after Clapper. *SCL Rev., 67*(3), 599–608. Retrieved from https://heinonline.org/HOL/Page?handle=hein.journals/sclr67&div=36&g_sent=1&casa_token=&collection=journals

Orb, A., Eisenhauer, L., & Wynaden, D. (2001). Ethics in qualitative research. *Journal of*

Nursing Scholarship, 33(1), 93–96. doi:10.1111/j.1547-5069.2001.00093.x

Origlia Ikhilor, P., Hasenberg, G., Kurth, E., Stocker Kalberer, B., Cignacco, E., & Pehlke-Milde, J. (2018). Barrier-free communication in maternity care of allophone migrants: BRIDGE study protocol. *Journal of Advanced Nursing, 74*(2), 472–481. doi:10.1111/jan.13441

Panahifar, F., & Shokouhyar, S. (2019). An interpretive structural modelling of enablers for collaborative planning, forecasting and replenishment implementation in high-tech industries. *International Journal of Information and Decision Sciences, 11*(1), 55–72. doi:10.1504/IJIDS.2019.096631

Paradis, E., O'Brien, B., Nimmon, L., Bandiera, G., & Martimianakis, M. A. (2016). Design: selection of data collection methods. *Journal of Graduate Medical Education, 8*(2), 263–264. doi:10.4300/JGME-D-16-00098.1

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making, 9*(2), 117–129. doi:10.1177/1555343415575152

Pawlowski, S. D., & Yoonhyuk, J. (2015). Social representations of cybersecurity by university students and implications for instructional design. *Journal of Information Systems Education, 26*(4), 281–294. Retrieved from https://eric.ed.gov/?id=EJ1113944

Percy, W. H., Kostere, K., & Kostere, S. (2015). Generic qualitative research in psychology. *The Qualitative Report, 20*(2), 76–85. Retrieved from

http://nsuworks.nova.edu/tqr/vol20/iss2/7

Peter, E. (2015). The ethics in qualitative health research: special considerations. *Ciência & Saúde Coletiva, 20*(9), 2625–2630. doi:10.1590/1413-81232015209.06762015

Petrova, E., Dewing, J., & Camilleri, M. (2016). Confidentiality in participatory research: Challenges from one study. *Nursing Ethics*, *23*(4), 442–454. doi:10.1177/0969733014564909

Prakash, M., & Singaravel, G. (2015). An approach for prevention of privacy breach and information leakage in sensitive data mining. *Computers & Electrical Engineering, 45*(1), 134–140. doi:10.1016/j.compeleceng.2015.01.016

Privacy Rights Clearinghouse. (2018). Privacy rights clearinghouse data breaches export [Data file]. Available from https://www.privacyrights.org/data-breaches

Privacy Rights Clearinghouse. (2020). Privacy rights clearinghouse data breaches export [Data file]. Available from https://www.privacyrights.org/data-breaches

Pryce, J., Lee, W., Crowe, E., Park, D., McCarthy, M., & Owens, G. (2019). A case study in public child welfare: County-level practices that address racial disparity in foster care placement. *Journal of Public Child Welfare, 13*(1), 35–59. doi:10.1080/15548732.2018.1467354

Qamar, B. K. (2018). Research ethics. *Pakistan Armed Forces Medical Journal, 68*(6), 1503–54. Retrieved from https://www.pafmj.org/index.php/PAFMJ/article/view/2381

Queirós, A., Faria, D., & Almeida, F. (2017). Strengths and limitations of qualitative and quantitative research methods. *European Journal of Education Studies*, *3*(9), 369–

387. doi:10.5281/zenodo.887089

Quick, J., & Hall, S. (2015). Part two: Qualitative research. *Journal of perioperative practice*, *25*(7–8), 129–133. doi:10.1177/1750458915025007-803

Ramsden, B. (2016). Ethnographic methods in academic libraries: A review. *New Review of Academic Librarianship*, *22*(4), 355–369. doi:10.1080/13614533.2016.1231696

Razmi-Farooji, A., Kropsu-Vehkaperä, H., Härkönen, J., & Haapasalo, H. (2019). Advantages and potential challenges of data management in e-maintenance. *Journal of Quality in Maintenance Engineering*, *25*(3), 378–396. doi:10.1108/JQME-03-2018-0018

Reece, R. P., & Stahl, B. C. (2015). The professionalisation of information security: Perspectives of UK practitioners. *Computers & Security*, *48*(C), 182–195. doi:10.1016/j.cose.2014.10.007

Refaei, B., Kumar, R., & Harmony, S. (2015). Working Collaboratively to Improve Students' Application of Critical Thinking to Information Literacy Skills. *Writing & Pedagogy*, *7*(1), 117–137. doi:10.1558/wap.v7i1.17232

Rizvi, S., Pipetti, R., McIntyre, N., & Todd, J. (2020). Threat model for securing internet of things (IoT) network at device-level. *Internet of Things*, 100240. doi:10.1016/j.iot.2020.100240

Rodriguez, M. (2018). HTTPS everywhere: Industry trends and the need for encryption. *Serials Review*, *44*(2), 131–137. doi:10.1080/00987913.2018.1472478

Ropret, M., Aristovnik, A., & Kovač, P. (2018). A content analysis of the rule of law

within public governance models: Old vs. new EU member states. *NISPAcee Journal of Public Administration and Policy, 11*(2), 129–152. doi:10.2478/nispa-2018-0016

Rosati, P., Deeney, P., Cummins, M., van der Werff, L., & Lynn, T. (2019). Social media and stock price reaction to data breach announcements: Evidence from US listed companies. *Research in International Business and Finance, 47*(C), 458–469. doi:10.1016/j.ribaf.2018.09.007

Rousseau, D. (2015). General systems theory: Its present and potential. *Systems Research And Behavioral Science, 32*(5), 522–533. doi:10.1002/sres.2354

Rousseau, D., Wilby, J., Billingham, J., & Blachfellner, S. (2016). The scope and range of general systems transdisciplinarity. *Systema: Connecting Matter, Life, Culture And Technology, 4*(1), 48–60. Retrieved from http://www.systema-journal.org/article/view/403

Rutberg, S., & Bouikidis, C. D. (2018). Focusing on the fundamentals: A simplistic differentiation between qualitative and quantitative research. *Nephrology Nursing Journal, 45*(2), 209–213. Retrieved from https://europepmc.org/abstract/med/30303640

Safa, N. S., von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*(C), 70–82. doi:10.1016/j.cose.2015.10.006

Sato, T., & Haegele, J. A. (2016). Graduate students' initial exploration of teaching students with disabilities in physical education. *International Journal of Special*

Education, 31(3), 1–31. Retrieved from https://eric.ed.gov/?id=EJ1120691

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., ... & Jinks, C. (2018). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity*, *52*(4), 1893–1907. doi:10.1007/s11135-017-0574-8

Saunders, F. C., Gale, A. W., & Sherry, A. H. (2016). Responding to project uncertainty: Evidence for high reliability practices in large-scale safety–critical projects. *International Journal of Project Management, 34*(7), 1252–1265. doi:10.1016/j.ijproman.2016.06.008

Schatz, D., & Bashroush, R. (2016). The impact of repeated data breach events on organisations' market value. *Information & Computer Security*, *24*(1), 73–92. doi:10.1108/ICS-03-2014-0020

Selvam, A. M. (2015). Universal spectrum for DNA Base CG frequency distribution in Takifugu Rubripes (Puffer Fish) genome. *Chaos and Complexity Letters, 9*(1), 15–42. Retrieved from https://urlzs.com/S9nYK

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems, 32*(2), 314–341. doi:10.1080/07421222.2015.1063315

Shaked, H., & Schechter, C. (2018). Holistic school leadership: Development of systems thinking in school leaders. *Teachers College Record, 120*(2), 1–59. Retrieved from https://www.tcrecord.org/Content.asp?ContentId=21964

Shaw, D. (2013). Rigour in qualitative case-study research. *Nurse Researcher, 20*(4), 12–

17. doi:10.7748/nr2013.03.20.4.12.e326

Short, M., Barton, H., Cooper, B., Woolven, M., Loos, M., & Devos, J. (2017). The power of the case study within practice, education and research. *Advances in Social Work and Welfare Education, 19*(1), 92–106. Retrieved from https://search.informit.com.au/documentSummary;dn=054289236281857;res=IELHSS

Shrivastava, S., Sonpar, K., & Pazzaglia, F. (2009). Normal accident theory versus high reliability theory: A resolution and call for an open systems view of accidents. *Human Relations, 62*(9), 1357–1390. doi:10.1177/0018726709339117

Smith, C. T., Hopkins, C., Sydes, M. R., Woolfall, K., Clarke, M., Murray, G., & Williamson, P. (2015). How should individual participant data (IPD) from publicly funded clinical trials be shared?. *BMC medicine, 13*(301), 1–7. doi:10.1186/s12916-015-0532-z

Sohou, A., & Holtkamp, P. (2018). Are users competent to comply with information security policies? An analysis of professional competence models. *Information Technology & People, 31*(5), 1047–1068. doi:10.1108/ITP-02-2017-0052

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*(2), 215–225. doi:10.1016/j.ijinfomgt.2015.11.009

Spears, J. L. (2018). Teaching tip: Gaining real-world experience in information security: A roadmap for a service-learning course. *Journal of Information Systems Education, 29*(4), 183–202. Retrieved from

https://aisel.aisnet.org/jise/vol29/iss4/1

Squires, A., & Dorsen, C. (2018). Qualitative research in nursing and health professions regulation. *Journal of Nursing Regulation*, *9*(3), 15–26. doi:10.1016/S2155-8256(18)30150-9

Stafford, T., Gal, G., Poston, R., Crossler, R. E., Jiang, R., & Lyons, R. (2018). The role of accounting and professional associations in it security auditing: An AMCIS panel report. *Communications of the Association for Information Systems*, *43*(1), 27. doi:10.17705/1CAIS.04327

Stillerman, J., Fredian, T., Greenwald, M., & Manduchi, G. (2016). Data catalog project—A browsable, searchable, metadata system. *Fusion Engineering and Design*, *112*, 995–998. doi:10.1016/j.fusengdes.2016.05.004

Sutton, J., & Austin, Z. (2015). Qualitative research: Data collection, analysis, and management. *The Canadian Journal of Hospital Pharmacy*, *68*(3), 226–231. Retrieved from https://www.cjhp-online.ca/cshp/index.php/cjhp/article/view/1456/2153

Taguchi, N. (2018). Description and explanation of pragmatic development: Quantitative, qualitative, and mixed methods research. *System*, *75*, 23–32. doi:10.1016/j.system.2018.03.010

Tariq, N., Asim, M., & Khan, F. A. (2019). Securing scada-based critical infrastructures: Challenges and open issues. *Procedia Computer Science*, *155*, 612–617. doi:10.1016/j.procs.2019.08.086

Teece, D. J. (2018). Dynamic capabilities as (workable) management systems theory.

Journal of Management & Organization, 24(3), 359–368. doi:10.1017/jmo.2017.75

Thompson, H. (2013). The human element of information security. *Security & Privacy, IEEE, 11*(1), 32–35. doi:10.1109/MSP.2012.161

Ubit, F., & Bartholomaeus, P. (2018). Teacher professional development at a tsunami-affected school in Banda Aceh. *International Education Journal: Comparative Perspectives, 17*(2), 102–114. Retrieved from https://openjournals.library.sydney.edu.au/index.php/IEJ

United States Department of Health and Human Services. (1979). The Belmont report: Ethical principles and guidelines for the protection of human subjects of research. Retrieved from http://ohsr.od.nih.gov/guidelines/belmont.html

van de Wetering, R., Mikalef, P., & Helms, R. (2017). Driving organizational sustainability-oriented innovation capabilities: A complex adaptive systems perspective. *Current Opinion in Environmental Sustainability, 28*, 71–79. doi:101016/j.cosust.2017.08.006

Varella, L. (2016). When it rains, it pours: Protecting student data stored in the cloud. *Rutgers Computer & Tech. LJ, 42*(1), 94–119. Retrieved from https://heinonline.org/HOL/P?h=hein.journals/rutcomt42&i=104

von Bertalanffy, L. (1950). The theory of open systems in physics and biology. *Science, 111*(2872), 23–29. Retrieved from http://www.jstor.org/stable/1676073

von Bertalanffy, L. (1972). The history and status of general systems theory. *Academy of Management Journal, 15*(4), 407–426. doi:10.2307/255139

von Bertalanffy, L. (2008). An outline of general system theory. *Emergence: Complexity & Organization, 10*(2), 103–123. doi:10.1093/bjps/I.2.134

Wang, Y., Shi, S., Nevo, S., Li, S., & Chen, Y. (2015). The interaction effect of IT assets and IT management on firm performance: A systems perspective. *International Journal Of Information Management, 35*(5), 80–593. doi:10.1016/j.ijinfomgt.2015.06.006

Weidman, J. and J. Grossklags (2018). What's in your policy? An analysis of the current state of information security policies in academic institutions. *Proceedings of ECIS 2018, European Conference on Information Systems*. Retrieved from https://aisel.aisnet.org/ecis2018_rp/23

Whitney, K., Bradley, J. M., Baugh, D. E., & Chesterman, C. W., Jr. (2015). Systems theory as a foundation for governance of complex systems. *International Journal of System of Systems Engineering, 6*(1–2), 15–32. doi:10.1504/IJSSE.2015.068805

Wilkinson, I. A., & Staley, B. (2019). On the pitfalls and promises of using mixed methods in literacy research: perceptions of reviewers. *Research Papers in Education, 34*(1), 61–83. doi:10.1080/02671522.2017.1402081

Woith, W. M., Kerber, C., Astroth, K. S., & Jenkins, S. H. (2017). Lessons from the homeless: civil and uncivil interactions with nurses, self-care behaviors, and barriers to care. *Nursing Forum, 52*(3), 211–220. doi:10.1111/nuf.12191

Wolgemuth, J. R., Erdil-Moody, Z., Opsal, T., Cross, J. E., Kaanta, T., Dickmann, E. M., & Colomer, S. (2015). Participants' experiences of the qualitative interview:

Considering the importance of research paradigms. *Qualitative Research, 15*(3), 351–372. doi:10.1177/1468794114524222

Woods, D., Agrafiotis, I., Nurse, J. R., & Creese, S. (2017). Mapping the coverage of security controls in cyber insurance proposal forms. *Journal of Internet Services and Applications, 8*(1), 8. doi:10.1186/s13174-017-0059-y

Yakhnich, L. (2016). "This is my responsibility": Parental experience of former Soviet Union immigrant parents in Israel. *International Journal of Child, Youth and Family Studies, 7*(1), 1–26. doi:10.18357/ijcyfs.71201615414

Yates, J., & Leggett, T. (2016). Qualitative research: An introduction. *Radiologic Technology, 88*(2), 225–231. Retrieved from https://europepmc.org/abstract/med/27837140

Yilmaz, R., & Yalman, Y. (2016). A comparative analysis of university information systems within the scope of the information security risks. *TEM Journal, 5*(2), 180–191. doi:10.18421/TEM52-10

Young, J. C., Rose, D. C., Mumby, H. S., Benitez-Capistros, F., Derrick, C. J., Finch, T., ... & Parkinson, S. (2018). A methodological guide to using and reporting on interviews in conservation science research. *Methods in Ecology and Evolution, 9*(1), 10–19. doi:10.1111/2041-210X.12828

Yurtseven, M. K., & Buchanan, W. W. (2016). Complexity decision making and general systems theory: An educational perspective. *Sociology Study, 6*(2), 77–95. doi:10.17265/2159-5526/2016.02.001

Zhu, R., & Janczewski, L. J. (2015). Typology of information systems security research:

A methodological perspective. *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)*, 93–98. doi:10.1109/InfoSec.2015.7435512

Appendix A: Interview Protocol

I. Data Custodian Interview Protocol

Date: _____

Time: _____

Institution: _____

Participant (Title/Name): _____

Location: _____

Interview Checklist:

_____ A: Consent Form

_____ B: Interview Background

_____ C: Demographic Questions

_____ D: Institutional Perspective

_____ E: Interview Questions

_____ F: Post Interview Conclusion and Questions

Additional Discussion(s):_____

_____

_____

_____

_____

_____

_____

Additional Documents Obtained: _____

_____

II. Introduction to research

A. Introductory Script/Consent Form

Hello! To make sure that the information you are providing is properly documented and later transcribed, I would like to audio tape our conversation today. Please fill out this consent form. For your information, only myself, and if need be, my doctoral committee, will be privy to the tapes which will be eventually destroyed after they are transcribed. This document states that: (1) all information will be held confidential, (2) that the information collected will be stored in a safe for 5 years, (3) your participation is voluntary and you may stop at any time if you feel uncomfortable, and (4) I do not intend to inflict any harm. Thank you for your agreeing to participate in this interview.

I have planned this interview to last no longer than one hour. During this time, I have several questions that we would like to cover. If we begin to run over the allotted time, I will inform you and we will make the necessary adjustments to make sure that all questions are answered and that you are able to present all relevant information to me in a timely manner.

After consent is received, the recording device will be started

B. Interview Background

I have asked you to speak with me today because you have been identified as someone who has the responsibility as a data custodian on this campus. My research project is looking to see what information security strategies do university data custodians use to protect PII collected from staff, students and other stakeholders. My study does not aim to find fault in anything occurring on the campus. Rather, I am trying to see if the security strategies set up at colleges and universities can be improved to further protect collected data.

C. Demographic Questions

The following questions are basic questions to get a feel for the level of expertise you have in your field. This information is purely demographic.

1. What is your current title and role/responsibilities at the university?

2. What role do you have in providing data security for the institution?

3. How long have you been providing data security for the university? For any institution?

4. What applicable data security certifications and/or training have you had or plan to obtain?

D. Institutional Perspective

Thank you for that information. Now can you please briefly give me some perspective on how you feel the university views, treats and protects collected data?

E. Interview Questions

Thank you for providing me with that information. I think it is important to open the floor with a candid response to set the tone for the next set of questions. Now I only have 10 questions and 1 follow up question. The follow up question will allot you the opportunity to give me any information that you feel I may not have touched on to properly address the research question.

1. What training is given to data custodians to aid in ensuring proper data security?
2. Does your university develop security strategies based on a particular framework or standard?
3. Does your university have a centralized or decentralized management structure for data custodians across campus?
4. Were you involved in the process for choosing which person(s) modify the implemented security strategies? If so, what is that process?
5. How have other university data breaches caused this university to amend its existing security strategies in the past 5 to 10 years?
6. In your experience, which security strategies have been the most beneficial in providing data security for the university? Why have they been the most beneficial?
7. How often are the university's security strategies updated?
8. What prompted the implementation of the security strategies that exist within the university today?
9. What external factors play a role in deciding what strategies to implement within the university? Do these external influences cause challenges or make it easier to implement these strategies?
10. What method is used to measure the effectiveness of the security strategies? Is this method used before, after or throughout implementation?

F. Post Interview Conclusion and Questions:

11. Do you have any additional information to provide surrounding security strategy implementation at the university that has not already been addressed?

Appendix B: Interview Questions

Demographic Questions

1. What is your current title and role/responsibilities at the university?

2. What role do you have in providing data security for the institution?

3. How long have you been providing data security for the university? For any institution?

4. What applicable data security certifications and/or training have you had or plan to obtain?

Interview Questions

1. What training is given to data custodians to aid in ensuring proper data security?

2. Does your university develop security strategies based on a particular framework or standard?

3. Does your university have a centralized or decentralized management structure for data custodians across campus?

4. Were you involved in the process for choosing which person(s) modify the implemented security strategies? If so, what is that process?

5. How have other university data breaches caused this university to amend its existing security strategies in the past 5 to 10 years?

6. In your experience, which security strategies have been the most beneficial in providing data security for the university? Why have they been the most beneficial?

7. How often are the university's security strategies updated?

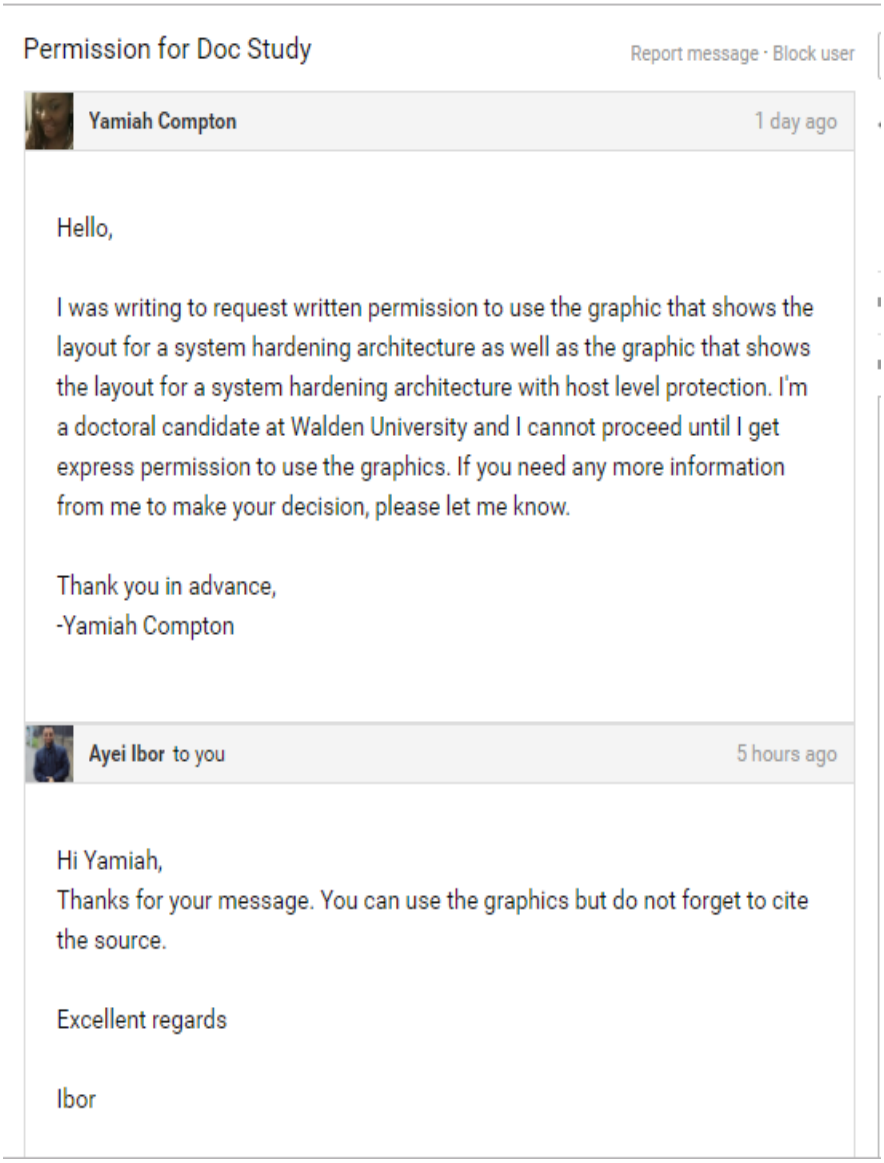
8. What prompted the implementation of the security strategies that exist within the university today?

9. What external factors play a role in deciding what strategies to implement within the university? Do these external influences cause challenges or make it easier to implement these strategies?

10. What method is used to measure the effectiveness of the security strategies? Is this method used before, after or throughout implementation?

11. Do you have any additional information to provide surrounding security strategy implementation at the university that has not already been addressed?

Appendix C: Permission to Use Graphics



Permission for Doc Study

Report message · Block user

Yamiah Compton 1 day ago

Hello,

I was writing to request written permission to use the graphic that shows the layout for a system hardening architecture as well as the graphic that shows the layout for a system hardening architecture with host level protection. I'm a doctoral candidate at Walden University and I cannot proceed until I get express permission to use the graphics. If you need any more information from me to make your decision, please let me know.

Thank you in advance,
-Yamiah Compton

Ayei Ibor to you 5 hours ago

Hi Yamiah,
Thanks for your message. You can use the graphics but do not forget to cite the source.

Excellent regards

Ibor

Yamiah Compton 13 hours ago

Hello,

I was writing to request written permission to use the SUV model depicting the seven categories and three levels used for question development. I'm a doctoral candidate at Walden University and I cannot proceed until I get express permission to use the graphic. If you need any more information from me to make your decision, please let me know.

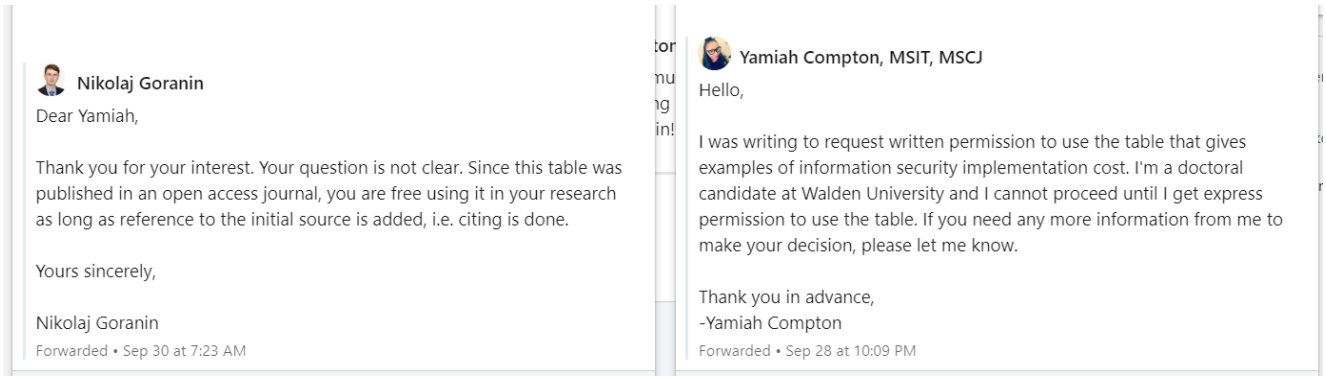
Thank you in advance,
-Yamiah Compton

Martin Thomas Östlund to you an hour ago

Hello Yamiah,

I have checked with my co-authors Päivi Jokela and Peter Karlsudd and you hereby have our consent to use the graphic representations of the SUV model in your research. We do not require any more information from you to grant this permission, but ask that you send a link to your finished work.

Best wishes och good luck with your research efforts
- Martin Östlund



Nikolaj Goranin

Dear Yamiah,

Thank you for your interest. Your question is not clear. Since this table was published in an open access journal, you are free using it in your research as long as reference to the initial source is added, i.e. citing is done.

Yours sincerely,

Nikolaj Goranin

Forwarded • Sep 30 at 7:23 AM

Yamiah Compton, MSIT, MSCJ

Hello,

I was writing to request written permission to use the table that gives examples of information security implementation cost. I'm a doctoral candidate at Walden University and I cannot proceed until I get express permission to use the table. If you need any more information from me to make your decision, please let me know.

Thank you in advance,
-Yamiah Compton

Forwarded • Sep 28 at 10:09 PM